

CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

UPDATED TABLE OF CONTENTS

RULEMAKING FILE

- Tab 1. Written Justification for Earlier Effective Date and Request for Expedited Review
- Tab 2. Notice of Proposed Rulemaking Action (NOPA)
- Tab 3. Original Proposed Regulations
- Tab 4. Initial Statement of Reasons (ISOR)
 - App A. (Standardized Regulatory Impact Analysis)
 - App B. (Department of Finance’s Comments)
- Tab 5. Statement of Mailing First 45-Day Notice
- Tab 6. First Notice of Modifications
- Tab 7. First Modified Regulations
- Tab 8. Statement of Mailing First 15-Day Notice
- Tab 9. Second Notice of Modifications
- Tab 10. Second Modified Regulations
- Tab 11. Statement of Mailing Second 15-Day Notice
- Tab 12. Public Comments
 - App A. (45-Day Written Comments)
 - App B. (First 15-Day Written Comments)
 - App C. (Second 15-Day Written Comments)
- Tab 13. Public Hearing Transcripts
 - App A. (Sacramento, December 2, 2019)
 - App B. (Los Angeles, December 3, 2019)
 - App C. (San Francisco, December 4, 2019)

App D. (Fresno, December 5, 2019)

Tab 14. Form 399 with Attachment

Tab 15. Materials / Documents Relied Upon

Appendix A. (Preliminary Activities)

Appendix B. (45-Day)

Appendix C. (15-Day)

Tab 16. Document Incorporated by Reference

Tab 17. Updated Informative Digest

Tab 18. Final Statement of Reasons (FSOR)

App A. Summary and Response to Comments Received in 45-Day Period

App B. List of Commenters from 45-Day Period

App C. Summary and Response to Comments Received in First 15-Day Period

App D. List of Commenters from First 15-Day Period

App E. Summary and Response to Comments Received in Second 15-Day Period

App F. List of Commenters from 2nd 15-Day Period

Tab 19. Addendum to Final Statement of Reasons

Tab 20. Third Notice of Modifications

Tab 21. Third Modified Regulations

Tab 22. Statement of Mailing of Third 15-Day Notice

Tab 23. Fourth Notice of Modifications

Tab 24. Fourth Modified Regulations

Tab 25. Statement of Mailing of Fourth 15-Day Notice

Tab 26. Additional Public Comments

App A. (Third 15-Day Written Comments)

App B. (Fourth 15-Day Written Comments)

Tab 27. Additional Materials / Documents Relied Upon (Fourth Notice)

Tab 28. Addendum to Updated Informative Digest

Tab 29. Second Addendum to Final Statement of Reasons (FSOR)

App G. Summary and Response to Comments Received in Third 15-Day Period

App H. List of Commenters from Third 15-Day Period

App I. Summary and Response to Comments Received in Fourth 15-Day Period

App J. List of Commenters from Fourth 15-Day Period

DECLARATION

I, Julia Zuffelato, am the agency official responsible for the compilation of this rulemaking file. The record in this matter was closed on June 1, 2020, and opened and closed again on August 13, 2020, and opened and closed again on January 26, 2021. The rulemaking as submitted is complete. I declare under penalty of perjury, under the laws of the State of California, that the foregoing is true and correct.

Executed on January 26, 2021, in Sacramento, California.



Julia Zuffelato
Deputy Attorney General

DEPARTMENT OF JUSTICE

Title 11. Law
Division 1. Attorney General
Chapter 20. California Consumer Privacy Act Regulations

October 12, 2020

**NOTICE OF THIRD SET OF PROPOSED MODIFICATIONS
TO TEXT OF REGULATIONS**
[OAL File No. 2019-1001-05]

Pursuant to the requirements of Government Code section 11346.8, subdivision (c), and section 44 of Title 1 of the California Code of Regulations, the California Department of Justice (Department) is providing notice of a third set of proposed modifications made to the regulations regarding the California Consumer Privacy Act.

The Department first published and noticed the proposed regulations for public comment on October 11, 2019. On February 10, 2020 and March 11, 2020, the Department gave notice of modifications to the proposed regulations, based on comments received during the relevant comment periods. The Department withdrew the following sections from the review of the Office Administrative Law (OAL) pursuant to Government Code section 11349.3, subd. (c): 999.305(a)(5), 999.306(b)(2), 999.315(c), and 999.326(c). OAL approved the other sections submitted by the Department, effective August 14, 2020, and these provisions became final.

The modifications are indicated by bold blue underline for proposed additions and red strike out for proposed deletions to the regulations that became effective on August 14, 2020. This third set of modifications include the following changes:

- Proposed section 999.306, subd. (b)(3), provides examples of how businesses that collect personal information in the course of interacting with consumers offline can provide the notice of right to opt-out of the sale of personal information through an offline method.
- Proposed section 999.315, subd. (h), provides guidance on how a business's methods for submitting requests to opt-out should be easy and require minimal steps. It provides illustrative examples of methods designed with the purpose or substantial effect of subverting or impairing a consumer's choice to opt-out.
- Proposed section 999.326, subd. (a), clarifies the proof that a business may require an authorized agent to provide, as well as what the business may require a consumer to do to verify their request.

-
- Proposed section 999.332, subd. (a), clarifies that businesses subject to either section 999.330, section 999.331, or both of these sections are required to include a description of the processes set forth in those sections in their privacy policies.

This Notice, the text of the third set of proposed modifications to the regulations, and a comparison of the text as approved by the Office of Administrative Law with the currently proposed modifications are available at www.oag.ca.gov/privacy/ccpa/current. The originally proposed regulations and all documents relating to the rulemaking package, including previous modifications to the proposed regulations, are also available at this website.

The Department will accept written comments regarding the proposed changes between Tuesday, October 13, 2020 and Wednesday, October 28, 2020. Please limit comments to the additions indicated in bold blue underline and the deletions indicated in red strike out. All written comments on the underlined changes must be submitted to the Department **no later than 5:00 p.m. on October 28, 2020** by email to PrivacyRegulations@doj.ca.gov, or by mail to the address listed below.

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

All timely comments received that are relevant to the third set of proposed modifications indicated in blue bold underline and red strike out format will be reviewed and responded to by the Department's staff as part of the compilation of the rulemaking file.

TEXT OF MODIFIED REGULATIONS

The Department first published and noticed the California Consumer Privacy Act (CCPA) regulations for public comment on October 11, 2019. On February 10, 2020 and March 11, 2020, the Department gave notice of modifications to the CCPA regulations. After submitting the CCPA regulations for review by the Office of Administrative Law (OAL), the Department withdrew certain provisions for further consideration. OAL approved the remainder of the CCPA regulations, which became effective August 14, 2020. The Department now proposes additional modifications to certain provisions of the approved CCPA regulations.

Changes to the CCPA regulations that became effective on August 14, 2020 are illustrated in **blue bold underline** for proposed additions and by ~~red-strikeout~~ for proposed deletions.

TITLE 11. LAW

DIVISION 1. ATTORNEY GENERAL

CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information.

(a) Purpose and General Principles

- (1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.
- (2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

- (b) A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows:
- (1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application’s settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business’s privacy policy that contains the same information.
 - (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out. That method shall comply with the requirements set forth in subsection (a)(2).
 - (3) A business that collects personal information in the course of interacting with consumers offline shall also provide notice by an offline method that facilitates consumers’ awareness of their right to opt-out. Illustrative examples follow:**
 - a. A business that collects personal information from consumers in a brick-and-mortar store may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.**
 - b. A business that collects personal information over the phone may provide the notice orally during the call where the information is collected.**
- (c) A business shall include the following in its notice of right to opt-out:
- (1) A description of the consumer’s right to opt-out of the sale of their personal information by the business;
 - (2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 999.315, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and
 - (3) Instructions for any other method by which the consumer may submit their request to opt-out.
- (d) A business does not need to provide a notice of right to opt-out if:
- (1) It does not sell personal information; and
 - (2) It states in its privacy policy that it does not sell personal information.
- (e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains the affirmative authorization of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.315 Requests to Opt-Out.

- (a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.
- (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.
- (c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.
 - (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.
 - (2) If a global privacy control conflicts with a consumer’s existing business-specific privacy setting or their participation in a business’s financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.
- (d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.
- (e) A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. If a business sells a consumer’s personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer’s information.

- (f) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. User-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.
- (g) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.
- (h) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:**
- (1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.**
- (2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.**
- (3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.**
- (4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.**
- (5) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.**

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 999.326 Authorized Agent.

- (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require ~~that~~ the ~~consumer~~ authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of ~~do~~ the following:
- ~~(1) Provide the authorized agent signed permission to do so.~~
 - ~~(2)~~(1) Verify their own identity directly with the business.
 - ~~(3)~~(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.
- (b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.
- (c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.
- (d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.332. Notices to Consumers Under 16 Years of Age.

- (a) A business subject to sections 999.330 and or 999.331 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

**STATEMENT OF 15-DAY NOTICE OF AVAILABILITY OF THIRD SET OF
MODIFICATIONS TO THE TEXT OF PROPOSED REGULATIONS**
(Section 44 of Title 1 of the California Code of Regulations)

On October 12, 2020, the Department of Justice mailed the third set of modifications to the text of the proposed regulations along with a notice of the public comment period to those persons specified in subsections (a)(1) through (4) of Section 44 of Title 1 of the CCR. The public comment period for the modified text was from October 13, 2020 through October 28, 2020.

DEPARTMENT OF JUSTICE

Title 11. Law
Division 1. Attorney General
Chapter 20. California Consumer Privacy Act Regulations

December 10, 2020

**NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT
OF REGULATIONS AND ADDITION OF DOCUMENTS AND
INFORMATION TO RULEMAKING FILE**

[OAL File No. 2019-1001-05]

Update to Proposed Text

Pursuant to the requirements of Government Code section 11346.8, subdivision (c), and section 44 of Title 1 of the California Code of Regulations, the California Department of Justice (Department) is providing notice of a fourth set of proposed modifications made to the regulations regarding the California Consumer Privacy Act.

The Department first published and noticed the proposed regulations for public comment on October 11, 2019. On February 10, 2020 and March 11, 2020, the Department gave notice of modifications to the proposed regulations, based on comments received during the relevant comment periods. The Department withdrew the following sections from the review of the Office Administrative Law (OAL) pursuant to Government Code section 11349.3, subd. (c): 999.305(a)(5), 999.306(b)(2), 999.315(c), and 999.326(c). OAL approved the other sections submitted by the Department, effective August 14, 2020, and these provisions became final.

On October 12, 2020, the Department gave notice of a third set of modifications on a number of provisions. Subsequently, the Department received around 20 comments in response to these modifications. This fourth set of modifications is in response to those comments and/or to clarify and conform the proposed regulations to existing law. The changes made include:

- Revisions to section 999.306, subd. (b)(3), to clarify that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of the sale of their personal information by an offline method.
- Proposed section 999.315, subd. (f), regarding a uniform button to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

This Notice and the text of the fourth set of proposed modifications to the regulations as compared with the text approved by the Office of Administrative Law are available at

www.oag.ca.gov/privacy/ccpa/current. The originally proposed regulations and all documents relating to the rulemaking package, including previous modifications to the proposed regulations, are also available at this website.

Update to Documents and Other Information Relied Upon

Pursuant to the requirements of Government Code sections 11346.8, subdivision (d), 11346.9, subdivision (a)(1), and 11347.1, the Department is also providing notice that documents and other information which the Department has relied upon in adopting the proposed regulations have been added to the rulemaking file and are available for public inspection and comment.

The documents and information added to the rulemaking file are as follows:

- Cranor, et al., *CCPA Opt-Out Icon Testing – Phase 2* (May 28, 2020).
- Habib, et al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019, August 11-13, 2019, Santa Clara, CA, USA. Available at https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-hana_habib.pdf.
- Habib, et al., “It’s a scavenger hunt”: Usability of Websites’ Opt-Out and Data Deletion Choices, CHI ’20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 2020, Honolulu, HI, USA. Available at https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-hana_habib.pdf (starting at page 21).
- Luguri, Jamie and Strahilevitz, Lior, *Shining a Light on Dark Patterns* (August 1, 2019), University of Chicago, Public Law Working Paper No. 719, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879.
- Mahoney, et al., *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?* (October 1, 2020), Consumer Reports. Available at https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

The entire rulemaking file, which includes the documents referenced above, is available for inspection and copying throughout the rulemaking process during business hours at the location listed below. In addition, the documents are available at <https://oag.ca.gov/privacy/ccpa/current>.

The Department will accept written comments regarding the proposed changes or materials added to the rulemaking file between Friday, December 11, 2020 and Monday, December 28, 2020. Please limit comments to the additions indicated in bold green double underline, the deletions indicated in red double strike out, and the documents added to the rulemaking file.

All written comments on the underlined changes must be submitted to the Department **no later than 5:00 p.m. on December 28, 2020** by email to PrivacyRegulations@doj.ca.gov, or by mail to the address listed below.

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

All timely comments received that pertain to the fourth set of proposed modifications or the new materials added will be reviewed and responded to by the Department's staff as part of the compilation of the rulemaking file.

TEXT OF MODIFIED REGULATIONS

The Department first published and noticed the California Consumer Privacy Act (CCPA) regulations for public comment on October 11, 2019. On February 10, 2020 and March 11, 2020, the Department gave notice of modifications to the CCPA regulations. After submitting the CCPA regulations for review by the Office of Administrative Law (OAL), the Department withdrew certain provisions for further consideration. OAL approved the remainder of the CCPA regulations, which became effective August 14, 2020. The Department now proposes additional modifications to certain provisions of the approved CCPA regulations.

Changes to the CCPA regulations that became effective on August 14, 2020 are illustrated in **blue bold underline** for proposed additions and by ~~red-strikeout~~ for proposed deletions. Additional changes made in response to comments received are illustrated in **green bold double underline** for proposed additions and by ~~red bold double strikeout~~ for proposed deletions.

TITLE 11. LAW

DIVISION 1. ATTORNEY GENERAL

CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information.

(a) Purpose and General Principles

- (1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.
- (2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other

contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(b) A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows:

(1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application’s settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business’s privacy policy that contains the same information.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out. That method shall comply with the requirements set forth in subsection (a)(2).

(3) A business that ~~sells~~ ~~collects~~ personal information that it collects in the course of interacting with consumers offline shall also ~~provide notice~~ inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request to opt-out ~~by an offline method that facilitates consumers’ awareness of their right to opt-out.~~ Illustrative examples follow:

a. A business that ~~sells~~ ~~collects~~ personal information that it collects from consumers in a brick-and-mortar store may ~~inform consumers of their right to opt-out~~ ~~provide notice by printing the notice~~ on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the ~~notice~~ ~~opt-out information~~ can be found online.

b. A business that ~~sells~~ ~~collects~~ personal information that it collects over the phone may ~~inform consumers of their right to opt-out~~ ~~provide the notice~~ orally during the call ~~where~~ ~~when~~ the information is collected.

(c) A business shall include the following in its notice of right to opt-out:

(1) A description of the consumer’s right to opt-out of the sale of their personal information by the business;

(2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 999.315, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and

(3) Instructions for any other method by which the consumer may submit their request to opt-out.

(d) A business does not need to provide a notice of right to opt-out if:

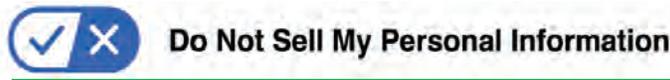
- (1) It does not sell personal information; and
 - (2) It states in its privacy policy that it does not sell personal information.
- (e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains the affirmative authorization of the consumer.

(f) Opt-Out Button.

(1) The following opt-out button may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations.



(2) Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button shall be added to the left of the text as demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link.



(3) The button shall be approximately the same size as any other buttons used by the business on its webpage.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.315 Requests to Opt-Out.

- (a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.
- (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.

- (c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.
- (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.
 - (2) If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.
- (d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.
- (e) A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.
- (f) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. User-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.
- (g) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.
- (h) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business**

shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:

- (1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.
- (2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.
- (3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.
- (4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.
- (5) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 999.326 Authorized Agent.

- (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require ~~that~~ the ~~consumer~~ authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of ~~do~~ the following:
 - ~~(1) Provide the authorized agent signed permission to do so.~~
 - ~~(2)~~(1) Verify their own identity directly with the business.
 - ~~(3)~~(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.
- (b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.

- (c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.
- (d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.332. Notices to Consumers Under 16 Years of Age.

- (a) A business subject to sections 999.330 and/or 999.331 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

**STATEMENT OF 15-DAY NOTICE OF AVAILABILITY OF FOURTH SET OF
MODIFICATIONS TO THE TEXT OF PROPOSED REGULATIONS
AND AVAILABILITY OF DOCUMENT AND INFORMATION**

(Section 44 of Title 1 of the California Code of Regulations; Government Code section 11347.1)

On December 10, 2020, the Department of Justice mailed the fourth set of modifications to the text of the proposed regulations along with a notice of the public comment period to those persons specified in subsections (a)(1) through (4) of Section 44 of Title 1 of the CCR. The Department of Justice also mailed notice that the documents and other information which the Department has relied upon in adopting the proposed regulations have been updated and are available for public inspection and comment. The notice described the documents and information and stated that these documents were available for public inspection at the California Office of the Attorney General located at 300 South Spring Street, First Floor, Los Angeles, CA 90013, during business hours. The notice advised that the public could comment on the modified text and the documents and information from December 11, 2020 through December 28, 2020.

From: [REDACTED]
To: [Privacy Regulations](#)
Subject: RE: Comment on proposed regulatory amendments
Date: Tuesday, October 13, 2020 2:43:22 AM

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

From: [REDACTED]
Sent: Monday, October 12, 2020 12:58 PM
To: 'PrivacyRegulations@doj.ca.gov' <PrivacyRegulations@doj.ca.gov>
Subject: Comment on proposed regulatory amendments

[REDACTED]

The proposed addition to § 999.315 seeks to further complicate the opt-out right regulations, which are already overreaching and invite fraud and abuse, by imposing an additional series of confusing stipulations that would make it significantly harder for online businesses to comply in good faith with the regulations.

First, the stipulation proposed in (h)(1) for counting a number of steps is confusing, nonsensical, and completely arbitrary. **It would significantly penalize, to no good purpose, businesses like mine that use webforms as a means of processing CCPA requests.** By setting an arbitrary standard for number of clicks or number of steps, this stipulation would arbitrarily penalize the use of CAPTCHAs or other means to ensure that the webform is being submitted by a human user rather than bots, who are drawn to webforms like moths to a flame. Since the regulations are written to require that businesses respond promptly to ALL requests, even obviously fraudulent ones, **this expectation would devastate small businesses like mine.** I have only modest online traffic, but if I post a webform without a CAPTCHA or other means of separating human users from bots, I may get HUNDREDS of obviously fraudulent spam submissions a day. As a sole proprietor, I simply do not

W377-1

have the time to handle that volume of responses.

W377-1
cont

Furthermore, this stipulation would effectively require that all means of submitting requests involve the same number of steps, which is obviously and fundamentally ridiculous. For a consumer who has an established ongoing relationship with a business -- for example, a customer who logs into an account with an online retailer -- the process of submitting an opt-in or opt-out request may be as simple as a single click on their account settings page; in that case, the business already knows who the consumer is and has mechanisms in place for managing their information. For a website visitor who does NOT have an established relationship with the business, they will almost certainly need to indicate to the business who they are (and that they're human) so that the business can respond to and process their request. Once a business has received an opt-out request from a given consumer, processing an opt-in-request from the same individual is an inherently simpler process.

W377-2

These procedures clearly, logically, NECESSARILY involve a different number of steps, so to stipulate that they not only shouldn't but may NOT by law require a different number of steps is absurd. That is not practical, practicable, or enforceable, and represents a further unwarranted overreach by OAG.

I strongly recommend that (h)(1) be struck in its entirety. If OAG attempts to revise the wording of this provision in an effort to clarify this mess, it's likely to compound rather than resolve the issues it presents.

The proposed example in (5)(h) is in some respects even more concerning. I grasp that the intent is to discourage businesses from "burying" opt-out instructions in voluminous text, but stipulating that "the business shall not require to search or scroll through the text of a privacy policy or similar document or webpage" would effectively allow OAG to set arbitrary, undefined expectations for what constitutes excessive "searching or scrolling." Even a fairly straightforward Do Not Sell My Personal Information webpage, containing specific instructions for submitting requests, may require a fair bit of scrolling if a consumer accesses the page from a mobile phone rather than a desktop computer. It also threatens to penalize businesses for minor technical errors, such as an anchor link (that is, a hyperlink pointing to a specific anchor at a specific position on a given webpage) that fails to correctly resolve due to connection issues beyond the business's reasonable control.

W377-3

I do not object in principle to the proposed text of section (h), but the illustrative examples offer a disturbing indication that OAG's intention is to find ways to arbitrarily penalize businesses for minor procedural issues. Many business are striving in good faith to meet the often confounding expectations established in these regulations, but OAG seems determined to make that as difficult as possible.

My recommendation is to strike (h)(1) and (h)(5) in their entirety.

Regarding the proposed addition to § 999.326, the proposed change is, refreshingly, a straightforward and sensible clarification of the existing text.

W377-4



From: [Adam Schwartz](#)
To: [Privacy Regulations](#)
Subject: EFF comments on proposed Cal DOJ regulations re CCPA (OAL file no. 2019-1001-05)
Date: Tuesday, October 20, 2020 12:46:38 PM
Attachments: [2020-10-20 - EFF comments re Cal DOJ proposed regs re dark patterns.pdf](#)

Salutations. EFF submits the attached comments in support of the "dark patterns" regulations proposed by the California DOJ at Section 999,315(h) of the third set of proposed modifications of CCPA regulations, published on October 12. Sincerely, -Adam

--

Adam Schwartz | Senior Staff Attorney
Electronic Frontier Foundation
815 Eddy St. | San Francisco, CA 94109

██████████ ██████████

Pronouns: he/him/his



October 20, 2020

BY EMAIL (PrivacyRegulations@doj.ca.gov)

Re: EFF comments on proposed Cal DOJ regulations on “dark patterns”
(OAL File No. 2019-1001-05)

Salutations:

The Electronic Frontier Foundation (EFF) writes in support of the proposed regulations from the California Department of Justice (DOJ) to protect against what are commonly called “dark patterns.” These are manipulative user experience designs that businesses use to trick consumers into surrendering their personal data. Specifically, we support the proposed regulations at Section 999.315(h), within the third set of proposed modifications of CCPA regulations, which the California DOJ published on October 12.

The California Consumer Privacy Act (CCPA) created a right of consumers to opt-out of the sale of their personal data. Businesses might use dark patterns to hamstring this CCPA right. The proposed DOJ regulations will secure this right by stopping dark patterns. Among other things, the proposed regulations would:

- Require opt-out processes to be “easy” and “require minimal steps.”
- Ban opt-out processes “designed with the purpose or having the substantial effect of subverting or impairing a consumer's choice to opt-out.”
- Limit the number of steps to opt-out to the number of steps to later opt back in.
- Ban “confusing language” such as “double negatives” (like “don’t not sell”).
- Ban the necessity to search or scroll through a document to find the opt-out button.

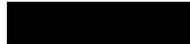
W378-1

For more on EFF’s opposition to dark patterns, please see:
eff.org/deeplinks/2019/02/designing-welcome-mats-invite-user-privacy-0.

For the DOJ’s proposed regulations, please see:
oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf

Sincerely,

Adam Schwartz
Senior Staff Attorney



From: [Zoe Vilain](#)
To: [Privacy Regulations](#)
Cc: [Pierre Valade](#)
Subject: To the attention of Deputy Attorney General Kim - Comments with regards to CCPA
Date: Tuesday, October 27, 2020 9:06:48 AM
Attachments: [20201027 - 2121 Atelier Inc - comments 3 on CCPA to California GA.pdf](#)

To the attention of Deputy Attorney General Kim

Dear Deputy Attorney General Kim,

Please find attached a letter to your attention containing our comments regarding the third set of proposed modifications to the CCPA regulation.

I am available for any queries,

Best regards,

Zoé Vilain

Jumbo Privacy

www.jumboprivacy.com



Jumbo Privacy
2121 Atelier Inc.
32 Bridge Street, 2nd Floor
Brooklyn, NY 11201
USA

Lisa B. Kim
Deputy Attorney General
California Department of Justice
Consumer Law Section – Privacy U.
300 South Spring Street, 1st Floor
Los Angeles, CA 90013
USA

October 27th, 2020

By email (privacyregulations@doj.ca.gov)

Subject: Written comments regarding the proposed CCPA regulations

Dear Deputy Attorney General Kim,

We write to you concerning the third set of proposed modifications to the California Consumer Privacy Act (“CCPA”) made on October 12th, 2020.

As mentioned in our previous letters to you dated respectively February 25, 2020, and March 27th, 2020, 2121 Atelier Inc. d/b/a Jumbo Privacy¹ has been acting as registered Authorized Agent in California for California residents, thanks to the introduction of such a role in the CCPA on Feb 1, 2020. Jumbo Privacy notably represents California consumers who request deletion of their personal information from consumer-selected businesses falling under the scope of the CCPA. Requests sent to a business by Jumbo Privacy on behalf of a consumer all contain the identification of the consumer and a signed mandate executed through and stored by a trusted third-party certifier, authorizing Jumbo to act on behalf of the consumer.

As of the date of this letter, 73% of businesses we are sending Requests to, are refusing to comply with our Requests based on the argument that such businesses refuse to comply with third-party requests to delete the personal information and/or require the consumer to take further action directly. Jumbo Privacy has therefore been pushing back against such refusals by quoting sections 1798-135 of the CCPA and § 999.315.e of the California Attorney General text of Regulations and indicating that such refusals are a restriction of consumer’s rights.

We are concerned that proposed modifications to the CCPA might highly restrict the efficiency and opportunity for consumers to mandate an Authorized Agent. Therefore, we are addressing once

¹ Available at <https://www.jumboprivacy.com/>

Jumbo Privacy
32 Bridge Street, 2nd Floor
Brooklyn, NY
11201

again our suggestions and comments to the proposed rulemakings of the California Attorney General regarding provisions related to the concept of “Authorized Agent”.

Specifically, our experience has demonstrated that every business falling under the scope of the CCPA should implement a dedicated communication channel with Authorized Agents, preferably an email address for the purpose of simplicity, to facilitate the management of requests made on behalf of consumers they represent. Indeed, if businesses force Authorized Agents to use web forms or postal mail, then Authorized Agents will not be able to manage privacy requests on behalf of their mandators efficiently. We also read proposed amendments to Section 999.326(1) and (3) to place unnecessary hurdles between Authorized Agents and the effective and efficient consumer control of private information.

W379-1

Consumers that mandate Jumbo Privacy as Authorized Agent to submit their requests are doing so to avoid having to manage such requests themselves, notably to avoid receiving numerous emails from businesses to confirm the validity of their requests or their identity. We believe that allowing a business to contact the consumer directly for additional identity verification after receipt of a request by mandate through an Authorized Agent, that has already verified the identification of the consumer, would lead to additional heavy processes and unnecessary delays to the processing of the original request.

W379-2

Security of personal information and verification of identity are a priority for Jumbo Privacy when acting as an Authorized Agent. We understand the importance of ensuring the validity of received requests to know or requests to delete. However, we would like to emphasize that providing an option for business to require the consumer verification of identity or request made through an agent might highly impair consumer rights by restraining the practicality to mandate an Authorized Agent.

We believe from requests we have made so far on behalf of consumers, that businesses may be tempted to use the presently proposed revisions to bypass an Authorized Agent’s authority to act on behalf of said consumers. Therefore, we would suggest these additions to ensure that businesses may verify a consumer’s identity only if the business can establish that the Authorized Agent has not provided reasonable proof of such consumer’s identity or the existence of a valid mandate. These additions would prevent any unnecessary verification by the business, ensuring respect of the consumer’s privacy rights.

W379-3

Regarding Article § 999.326 - Authorized Agent, please find below our proposed amendments highlighted in yellow below:

« (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require ~~that~~ the ~~consumer~~ **authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of ~~do~~** the following:

~~(1) Provide the authorized agent signed permission to do so.~~

(2)(1) Verify their own identity directly with the business in case the authorized agent has not provided reasonable proof that the authorized agent has previously verified the consumer's identity.

(3)(2) Directly confirm with the business that they provided the authorized agent permission to submit the request in case the authorized agent has not provided reasonable proof of the existence of the signed mandate.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.

(c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

(d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention. »

We remain of course at your disposal for any query,

Sincerely,

Zoé Vilain



Chief Privacy and Strategy Officer
Jumbo Privacy

Cc: Stacey Schesser, Supervising Deputy Attorney General
Privacy Regulations Coordinator, California Department of Justice

W379-3
cont

From: [Eric Ellman](#)
To: [Privacy Regulations](#)
Subject: Third Set of Proposed Modifications
Date: Tuesday, October 27, 2020 5:40:24 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.png](#)
[CCPA Regulations Comment Letter Third Set of Modifications.pdf](#)

To Whom It May Concern,

On behalf of the Consumer Data Industry Association, please find attached CDIA's comment on the Department of Justice's [Third Set of Proposed Modifications](#) to CCPA Regulations.

Respectfully submitted,
Eric J. Ellman

.....
Eric J. Ellman | [Senior Vice President, Public Policy and Legal Affairs](#) | Consumer Data Industry Association | Direct: [REDACTED] | [REDACTED] | 1090 Vermont Ave., NW, Suite 200, Washington, DC 20005, USA | CDIA: Empowering Economic Opportunity | Founded in 1906 | Please visit our blogs, [Federal Review](#), [Judicial Review](#), and the [Background Screening Information Center \(BaSIC\)](#)





Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: [REDACTED]

CDIAONLINE.ORG

October 28, 2020

Via Electronic Delivery to privacyregulations@doj.ca.gov

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring St., First Floor
Los Angeles, CA 90013

RE: Third Set of Modifications to California Consumer Protection Act Regulations

Dear Ms. Kim,

The Consumer Data Industry Association submits this comment letter in response to the California Office of the Attorney General's Third Set of Proposed Modifications to the California Consumer Privacy Act ("CCPA") Regulations.

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others.

CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies, including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA appreciates the thorough work of the Department of Justice (“Department” or “DOJ”) in finalizing the CCPA regulations. However, CDIA has serious concerns regarding the second grouping of proposed changes in this third set of modifications, specifically the changes to section 999.315(h) relating to opt-out requests. As we describe in greater detail below, the “illustrative examples” actually impose restrictions that do not implement any particular provision in the CCPA or the implementing regulations and exceed the law’s authorization for the Department to adopt regulations “*necessary* to further the purposes of” the law. See Cal. Civ. Code § 1798.185(b)(2) (emphasis added).

Additionally, imposing new requirements and restrictions with little notice makes compliance with those requirements very difficult from an operational standpoint. CDIA therefore respectfully requests at least 6 months of delayed enforcement on any changes the DOJ adopts.

To assist your office in promulgating clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on proposed section 999.315(h).

* * *

In this third set of proposed modifications to the CCPA regulations, the Department proposes to require that the methods for opting out must be “easy for consumers to execute and . . . require minimal steps to allow the consumer to opt-out.” The proposal also would prohibit use of a method designed with the purpose or that has the substantial effect of subverting or impairing a consumer’s choice to opt out.

The proposal then sets out what it refers to as “illustrative examples” of these two principles. However, the “illustrative examples” do not read as examples of methods that would or would not be easy to execute and require minimal steps to effective. Instead, the “examples” read as new requirements and restrictions not contemplated by the statute, that are not “necessary to further the purposes of the statute,” and that are otherwise problematic to the goals of the CCPA.

1. The proposed restriction that the number steps to opt out may not exceed the number of steps to opt in.

First, the proposal includes an illustrative example providing that a business's opt out method may not require more steps than the business's opt in process. The example also provides specifics as to how to count the steps to compare the two processes.

ISSUES: This proposal is not just an illustrative example but a strict limitation on how a business may set up its opt out and opt in processes, demonstrated by the strict guidance on how to "count" how many steps a process has. This is a specific restriction on the form businesses may use to receive verifiable consumer requests not contemplated in the statute or current regulations.

W380-1

Additionally, this restriction conflicts with existing regulation section 999.315(b), which provides that businesses must consider the methods by which they interact with consumers *along with* ease of use for the consumer. Businesses that deal in sensitive consumer information, like CDIA members, have established systems by which they interact with consumers, and a requirement to minimize the number of steps in submitting a request conflicts with the requirement to consider both ease of use *and* the normal methods of interaction.

PROPOSED SOLUTION: Replace the limitation on the number of steps a business may use in its opt out process with an instruction that for purposes of section 999.315(b), "ease of use by the consumer" includes considering the number of steps an opt out process takes.

2. The restriction that the opt-out method may not use double negatives or other "confusing language."

The second proposed illustrative example provides that a business may not use "confusing language, such as double-negatives" in the opt out process.

ISSUES: Banning "confusing language" is an overbroad prohibition lacking authorization in the statute.

W380-2

Additionally, other than noting that double negatives are confusing, this illustrative example provides no guidance as to what is or could be "confusing" to consumers. Prohibiting an undefined category of language thus raises due process concerns. Similarly, prohibiting an undefined category of speech also raises serious First Amendment concerns.

PROPOSED SOLUTION: Strike this section.

3. The restriction that a business may not require consumers to click through or listen to reasons not to opt out.

The third illustrative example prohibits business from requiring consumers to click through or listen to reasons not to opt out.

ISSUES: This is a prohibition on content a business may include in its opt out flow, not an illustrative example of “ease of use.” The CCPA opt out right only applies to certain data, for example, and a business should be able to educate a consumer about what effect an opt out does, and does not, have. Additionally, consumers might not understand the nature of the right, such as confusing the CCPA “opt out” with the FCRA’s prescreen opt out, which applies to data to which the CCPA opt out does not apply. If a consumer was seeking to exercise their federal right to opt out of prescreened solicitations, for example, CDIA members should be permitted to explain to a consumer that exercising their CCPA opt out right would not have the same effect. Without specific definitions or limitations, this prohibition could discourage businesses from including helpful, explanatory language that could help consumers navigate their choices under the CCPA.

W380-3

Furthermore, as a content restriction without any guidance on what it means by “reasons not to opt out,” this prohibition also raises serious due process and First Amendment concerns.

W380-4

PROPOSED SOLUTION: Strike this section.

4. The restriction that the business may not require a consumer to provide personal information not necessary to implement the request.

The fourth illustrative example provides that a business may not require in its opt out process that the consumer provide personal information “not necessary to implement the request.”

W380-5

ISSUES: The CCPA does not restrict what information a business can request in order to effectuate a consumer’s opt out, so this restriction exceeds the scope of the statute. The CCPA already prohibits, at Cal. Civ. Code § 1798.130(a)(7), a business from using personal information obtained for verification of a request for any purpose other than verification.

Additionally, CDIA has due process concerns with this restriction, as there is no guidance on how a business is expected to assess whether a particular data point is or is not necessary to implement a request on an individual, let alone a global, scale.

W380-6

Finally, businesses have to endeavor to match opt out requests to data on a particular consumer, and imposing a restriction on required data points complicates that mandate because matching is not always a straightforward task, given the variety of data that companies may collect and the variety of fields that data may contain. A business may be able

to improve its ability to match if it requests more data points. Without guidance as to what information the AG considers to be “not necessary” for this process, however, there is no way for a company to assess whether they comply with this standard.

W380-6
cont

PROPOSED SOLUTION: Strike this section.

- 5. The restriction that the business may not require a consumer to search or scroll through the text of a “privacy policy or similar document or webpage” to locate the opt-out mechanism.**

The fifth illustrative example provides that a business may not require a consumer to search or scroll through the text of “a privacy policy or similar document or webpage” to exercise an opt out.

ISSUES: This proposal is confusing, as it is not clear what counts as “a privacy policy or similar document or website.” The CCPA statute and current regulations already provides guidance on the placement of the Do Not Sell My Personal Information link.

W380-7

Furthermore, prohibiting the inclusion of information alongside the opt out mechanism raises serious due process and First Amendment concerns. Without clarity as to what the AG finds objectionable, businesses are not equipped to comply with this restriction.

PROPOSED SOLUTION: Strike this section.

* * *

Thank you for the opportunity to share its views on the proposed regulations. Please contact us if you have any questions or need further information based on comments.

Sincerely,



Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

From: [MacGregor, Melissa](#)
To: [Privacy Regulations](#)
Subject: SIFMA Letter to California AG re CCPA 3rd Amendments
Date: Wednesday, October 28, 2020 7:11:47 AM
Attachments: [SIFMA Letter to California AG re CCPA 3rd Amendments.pdf](#)

Please see the attached letter regarding the third proposed amendments to the CCPA regulations.

Please let me know if you have any questions.

Thanks.



October 28, 2020

VIA EMAIL TO: privacyregulations@doj.ca.gov
The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Proposed 3rd Amendment to California Consumer Privacy Act Regulations

Dear Attorney General Becerra,

The Securities Industry and Financial Markets Association (“SIFMA”)¹ appreciates this opportunity to comment on the third set of proposed modifications to the text of the California Consumer Privacy Act (“CCPA”) regulations. SIFMA commends your office for closely reviewing comments and making necessary changes when warranted. SIFMA previously submitted comments on the proposed CCPA regulations last December.²

While SIFMA commends the additional clarity in § 999.315, we believe that subsection (H)(1) is potentially confusing and subjective. We appreciate the principle that it must be equally easy to opt-in or out-out of the sale of personal information, but by including the language “opt-in to the sale of personal information after having previously opted out,” the Department may be inadvertently creating confusion. We request that the language be simplified to only address customers’ opt-in or opt-out actions and be consistent throughout the paragraph. Additionally, it is difficult to identify the “first indication by the

W381-1

W381-2

¹ SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry’s nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

² SIFMA Comment Letter to The Honorable Xavier Becerra dated December 6, 2019 (available at <https://www.sifma.org/resources/submissions/proposed-california-consumer-privacy-act-regulations-ccpa-rules/>).

consumer to the business of their interest to opt-in.” We request that the Department remove this language and replace it with “a request to opt-in is measured from when the consumer clicks to consent to opt-in.” This would bring the opt-in language in line with the opt-out language and remove the ambiguity around “first indication...of their interest” as that can be judged in multiple ways.

W381-2
cont

SIFMA greatly appreciates the consideration of these issues and would be pleased to discuss these comments in greater detail. If you have any questions or need any additional information, please contact me at [REDACTED].

Sincerely,

Melissa MacGregor
Managing Director & Associate General Counsel

cc: Kimberly Chamberlain, Managing Director & Associate General Counsel, SIFMA

From: [Maureen Mahoney](#)
To: [Privacy Regulations](#)
Subject: CR comments on third set of proposed modifications to the CCPA regs
Date: Wednesday, October 28, 2020 9:52:03 AM
Attachments: [CR Comments on 3rd Set of Modifications to CCPA Regs.pdf](#)
[CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf](#)

Dear Ms. Kim,

Attached, please see Consumer Reports' comments on the third set of modifications to the proposed CCPA regulations. I've also attached CR's recent report, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* which I'd like to submit to the record as well.

Please let me know if you need any additional information, and thank you for your help -

Best,
Maureen

--

Maureen Mahoney, Ph.D.
Policy Analyst

o [REDACTED] m [REDACTED]

[CR.org](#)



PLEASE NOTE: My email address has changed. Please begin using [REDACTED] for all future correspondence.

This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.



October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act (CCPA)

Dear Ms. Kim,

Consumer Reports¹ appreciates the opportunity to submit comments in response to the Notice of the Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act.² We welcome these proposed changes, especially those prohibiting the use of dark patterns—methods that substantially interfere with consumers’ efforts to opt out of the sale of their information.³ Consumer Reports has recently documented that some consumers are finding it very difficult to opt out of the sale of their information.⁴ In our recent study, over 500 consumers submitted opt-out requests to companies listed on the California data broker registry. Many of them encountered challenges: opt-out links too often were missing from the home page or difficult to find; opt-out processes were unnecessarily complicated, and companies asked consumers to submit sensitive information to verify their identities. In response, consumers sent over 5,000 messages to the AG, urging him to step up enforcement efforts and close up

W382-1

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

² California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Oct. 12, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf>.

³ *Id.* at §999.315(h)(1)-(5).

⁴ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers’ Rights Protected?*, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

loopholes in the CCPA that companies have exploited. The guidance on opt outs, including the prohibition on dark patterns, in this latest proposal will go a long way to addressing these problems. But more work is needed to ensure that consumers can properly exercise their privacy rights. We recommend that the AG:

W382-1
cont

- Finalize the proposed guidance on opt outs, including the prohibition on dark patterns;
- Finalize a design for the opt-out button;
- Require companies to confirm that they have honored opt-out requests;
- Finalize the authorized agent provisions as proposed;
- Close up loopholes in the definition of sale and tighten protections with respect to service providers, to ensure that consumers can opt out of behavioral advertising;
- Clarify that financial incentives in markets that lack competition is an unfair and usurious practice; and
- Establish a non-exclusive list of browser privacy signals that shall be honored as a universal opt out of sale.

Below, we explain these points in more detail.

The AG should finalize the proposed guidance on opt outs, including the prohibition on dark patterns.

We appreciate that the AG has proposed to “require minimal steps to allow the consumer to opt-out” and to prohibit dark patterns, in other words, “a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer’s choice to opt-out.”⁵ These regulations are essential given the difficulties that consumers have experienced in attempting to stop the sale of their information.

W382-1
cont

Subverting consumer intent online has become a real problem, and it’s important to address. In response to Europe’s recent GDPR privacy law, many websites forced users through confusing consent dialogs to ostensibly obtain consent to share and collect data for any number of undisclosed purposes.⁶ And researchers increasingly have been paying attention to manipulative dark patterns as well. A 2019 Princeton University study of 11,000 shopping sites found more than 1,800 examples of dark patterns, many of which clearly crossed the line into illegal deception.⁷

⁵ § 999.315(h).

⁶ *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

⁷ Mathur, Arunesh and Acar, Gunes and Friedman, Michael and Lucherini, Elena and Mayer, Jonathan and Chetty, Marshini and Narayanan, Arvind, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. (2019), <https://webtransparency.cs.princeton.edu/dark-patterns/>.

Use of these dark patterns is already illegal under Unfair and Deceptive Acts and Practices (UDAP) law, but that hasn't been adequate to protect consumers from these deceptive interfaces. For example, the Federal Trade Commission (FTC) sued Age of Learning, an online education service for children, for its deceptive interface that led consumers to believe they were signing up for one year of service, when in fact, by default, they were charged each year.⁸ Attorney General Karl Racine of the District of Columbia recently filed suit against Instacart for using a deceptive interface that made a service fee look like a tip.⁹ Last year, the FTC alleged that Match.com tricked consumers into subscribing by sending them misleading advertisements that claimed that someone wanted to date them—even though many of those communications were from fake profiles.¹⁰ Similarly, in late 2016, the FTC took action against Ashley Madison for using fake profiles to trick consumers into upgrading their membership.¹¹ The FTC took action against Facebook in 2011 for forcing consumers to use a deceptive interface to get them to provide so-called “consent” to share more data.¹² Despite these enforcement actions, the use of dark patterns remains all too common. Given how widespread these interfaces are, it's important to explicitly clarify that they are illegal in the CCPA context.

The proposed rules appropriately rein in the number of allowable steps to opt out.

We appreciate that the proposed rules limit the number of allowable steps in the opt-out process.¹³ As we noted in our recent study, some “Do Not Sell” processes involved multiple, complicated steps to opt out, including downloading third-party software, raising serious questions about the workability of the CCPA for consumers. For example, the data broker Outbrain doesn't have a “Do Not Sell My Personal Information” link on its homepage. The

⁸ Fed. Trade Comm'n v. Age of Learning, Inc., Complaint for Permanent Injunction and Other Equitable Relief, Case No. 2:20-cv-7996. U.S. District Court Central District of California at 4-6 (Sept. 1, 2020), <https://www.ftc.gov/system/files/documents/cases/1723086abcmousecomplaint.pdf>. According to the FTC, this is a UDAP violation, *See* ¶ 57.

⁹ District of Columbia v. Maplebear, Inc. d/b/a Instacart, Complaint for Violations of the Consumer Protection Procedures Act and Sales Tax Law, Superior Court of the District of Columbia at ¶ 2 (Aug. 2020), <https://oag.dc.gov/sites/default/files/2020-08/Instacart-Complaint.pdf>. The AG alleged that “Instacart’s misrepresentations and omissions regarding its service fee constitute deceptive and unfair trade practices that violated D.C. Code § 28-3904.” *See* ¶ 86.

¹⁰ Fed. Trade Comm'n v. Match Group, Inc., Complaint for Permanent Injunction, Civil Penalties, and Other Relief, Case No. 3:19-cv-02281, U.S. District Court, Northern District of Texas, Dallas Division at 2 (Sept. 25, 2019), https://www.ftc.gov/system/files/documents/cases/match_-_complaint.pdf. According to the FTC, this is a Section 5 violation. *See* p. 20-21.

¹¹ Fed. Trade Comm'n v. Ruby Corp. et al, Complaint for Permanent Injunction and Other Equitable Relief, Case 1:16-cv-02438, United States Circuit Court for the District of Columbia at 6 (Dec. 14, 2016), (<https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf>). According to the FTC, this is a Section 5 violation. *See* p. 13-14.

¹² Fed. Trade Comm'n, In the Matter of Facebook Inc. at 5-6 (2011) <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>. According to the FTC, this is a Section 5 violation. *See* p. 19.

¹³ § 999.315(h)(1).

consumer can click on the “Privacy Policy” link at the bottom of the page, which sends the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer can cut out several steps by clicking on “Interest-Based Ads” on the homepage.) If a consumer would like to opt out on their phone, they would have to go through another process. And if the consumer clears their cookies, they would need to opt out again. As one consumer told us, “It was not simple and required reading the ‘fine print.’” The proposed rules should help address this problem.

The proposed rules correctly prohibit companies from asking for unnecessary information to opt out.

We also appreciate the guidance that opt-out processes “shall not require the consumer to provide personal information that is not necessary to implement the request.”¹⁴ In our study, participants reported that they gave up the opt-out request 7% of the time. The overwhelming reason for a consumer to refrain from part of a DNS request process, or give up all together, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: “I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty.” Even consumers that ended up providing the drivers’ license ended up confused by the company’s follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: “After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that ‘[w]e will update the ranges in the future release.’ I have no idea what that means.” Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.

This information is clearly not necessary, as most data brokers simply requested name, address, and email. Unnecessary collection of sensitive data has significantly interfered with consumers’ ability to exercise their rights under the CCPA, and we appreciate that the proposed rules explicitly prohibit this.

¹⁴ § 999.315(h)(4).

The draft rules correctly stop businesses for making consumers search through a privacy policy to opt out.

We are also pleased that the draft rules preclude businesses from requiring consumers to dig through privacy policies to opt out.¹⁵ In our study, in some cases, consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, “There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart.” Another said of Oracle America, “The directions for opting out were in the middle of a wordy document written in small, tight font.” Another found the legal language used by Adrea Rubin Marketing intimidating: “they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury.”

W382-1
cont

Another data broker, ACBJ, placed a “Your California Privacy Rights” link at the bottom of their homepage (rather than a “Do Not Sell My Personal Information” link), which led to their privacy and cookie policy.¹⁶ Once on the policy page, the consumer is forced to search in their browser for the phrase “Do Not Sell My Personal Information” or scroll and scan ten sections of the privacy policy to find the paragraph with a “Do Not Sell My Personal Information” link, or follow two additional links to navigate from the privacy policy table of contents to the “Do Not Sell My Personal Information” link. Upon clicking the “Do Not Sell My Personal Information” link, the consumer is shown a pop-up with a page of additional legal information, and then has to scroll down to a toggle that finally allows them to request their data not be sold. In light of these reports from consumers, we urge the AG to finalize the prohibition on these practices.

The AG should finalize a design for the opt-out button.

Given that many consumers found it difficult to find the Do Not Sell link—it was often labeled with something different, and often buried at the bottom of the page with other links—a standardized graphic button would likely have value in ensuring that consumers would take advantage of that privacy protection. The CCPA directs the AG to design an opt-out button: “a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.”¹⁷ While the original design came under a fair amount of criticism, a uniform button will likely help consumers seeking to opt out, and the AG should promulgate one as soon as possible.

W382-2

¹⁵ § 999.315(h)(5).

¹⁶ ACBJ (last visited Oct. 28, 2020), <https://acbj.com/privacy#X>.

¹⁷ Cal. Civ. Code § 1798.185(a)(4)(C).

The AG should require companies to confirm that they have honored opt-out signals.

In our study, many consumers had no idea whether or not their opt-out request had been honored. The uncertainty often left consumers dissatisfied with the opt out. Some companies did notify consumers that their requests had been honored, and this information was characteristic of simple, quick, and effective opt-out processes.

Only in 18% of requests did participants report a clear confirmation from the broker that their data was or would soon not be sold. In 46% of tests, participants were left waiting or unsure about the status of their DNS request. In the 131 cases where the consumer was still waiting after one week, 82% were dissatisfied with the process (60% reported being very dissatisfied, and 22% reported being somewhat dissatisfied). The lack of clarity and closure was reflected in consumer comments such as “left me with no understanding of whether or not anything is going to happen” and “While it was an easy process—I will read their privacy policy to see if there is more [I] have to do to verify they are complying with my request. They left me unsure of the next step.”

W382-3

The AG should approve the proposed adjustment to the authorized agent provisions.

The authorized agent provisions are an essential part of the CCPA, and Consumer Reports has recently launched a pilot program to perform opt-out requests on consumers’ behalf.¹⁸ The CCPA puts far too much burden on individuals to safeguard their privacy; being able to designate an authorized agent to act on consumers’ behalf can help reduce that burden. The draft regulations support the work of authorized agents submitting access, deletion, and opt-out requests on consumers’ behalf, while ensuring that consumers’ privacy and security is protected.

While the CCPA pointedly does not require identity verification for opt-out requests, access and deletion requests have strong identity verification requirements. The regulations make it appropriately clear that a business may require additional identity verification, but not if the authorized agent can present proof that it holds a power of attorney from the consumer.¹⁹ If multiple companies required a consumer to submit additional identity verification, the authorized agent provision would no longer be practical for consumers. Obtaining a single power of attorney is easier and more efficient than going through many identity verification steps. Industry standards and standard form powers of attorney will make access and deletion pragmatic for the consumer, like the authorized agent opt-out process is currently.

W382-4

¹⁸ Ginny Fahs, *Putting the CCPA Into Practice: Piloting a CR Authorized Agent*, DIGITAL LAB AT CONSUMER REPORTS (Oct. 19, 2020), <https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8>.

¹⁹ § 999.326(b)

The regulations also require companies to honor valid opt-out requests from an authorized agent unless they have a “good-faith, reasonable, and documented belief that a request to opt-out is fraudulent.”²⁰ With these guidelines, an authorized agent that uses industry-standard verification of a consumer’s email address or telephone number will be able to complete an opt out without requiring consumers to provide hundreds, if not thousands, of verifications. This language allows companies to reject fraudulent opt outs without putting additional verification burdens on a consumer using a legitimate authorized agent.

W382-4
cont

The AG should clarify the definition of sale and tighten protections with respect to service providers, to ensure that consumers can opt out of behavioral advertising.

Many tech companies have exploited ambiguities in the definition of sale and the rules surrounding service providers to ignore consumers’ requests to opt out of behavioral advertising.²¹ Companies such as Spotify and Amazon claim that they are not “selling” data and that consumers can’t opt out of these data transfers—even though they share it with their advertising partners.²² Some companies claim that because data is not necessarily transferred for money, it does not constitute a sale.²³ But addressing targeted advertising is one of the main goals of the CCPA, which has an inclusive definition of personal information and a broad definition of sale to cover transfers of data for these purposes.²⁴

W382-5

Given the extent of the non-compliance, the AG should exercise its broad authority to issue rules to further the privacy intent of the Act,²⁵ and clarify that the transfer of data between unrelated companies for any commercial purpose falls under the definition of sale. This will help ensure that consumers can opt out of cross-context targeted advertising. We suggest adding a new definition to § 999.301:

“Sale” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s |

²⁰ § 999.315(g)

²¹ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, DIGITAL LAB AT CONSUMER REPORTS (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>.

²² Spotify, “Additional California Privacy Disclosures,” (July 1, 2020), <https://www.spotify.com/us/legal/california-privacy-disclosure/?language=en&country=us>; Amazon.com Privacy Notice,” (January 1, 2020), https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_FE2374D302994717AB1A8CE585E7E8BE.

²³ Tim Peterson, *‘We’re Not Going to Play Around’: Ad Industry Grapples with California’s Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), <https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/>.

²⁴ Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>; Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(t).

²⁵ Cal. Civ. Code § 1798.185(a).

personal information by the business to another business or a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

Another common way for companies to avoid honoring consumers' right to opt out of behavioral advertising is by claiming a service provider exemption. For example, the Interactive Advertising Bureau (IAB), a trade group that represents the ad tech industry, developed a framework for companies to evade the opt out by abusing a provision in the CCPA meant to permit a company to perform certain limited services on its behalf.²⁶

To address this problem, the AG should clarify that companies cannot transfer data to service providers for behavioral advertising if the consumer has opted out of sale. We reiterate our calls for a new .314(d):

If a consumer has opted out of the sale of their data, a company shall not share personal data with a service provider for the purpose of delivering cross-context behavioral advertising. "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

W382-5
cont

Additionally, the AG should take action to stop companies from combining data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they're just service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets. The AG has appropriately removed language in an earlier draft, which held that service providers can merge data across clients. But in the absence of a specific prohibition, given its disregard for the FTC consent order, Facebook (and other companies) will likely continue to engage in this behavior. The AG needs to make clear that this is not acceptable. We suggest the following language:

A service provider may not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

²⁶ *IAB CCPA Compliance Framework for Publishers & Technology Companies*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf.

Google and Facebook provide app developers privileged, valuable information—your data—in return for services that help increase engagement with their platforms.²⁷ The AG should refine the regulations in order to give consumers more control over their data with respect to these practices.

W382-5
cont

The AG should clarify that financial incentives in markets that lack competition is an unfair and usurious practice.

Californians have a right to privacy under the California Constitution, and consumers shouldn't be charged for exercising those rights. Unfortunately, there is contradictory language in the CCPA that could give companies the ability to charge consumers more for opting out of the sale of their data or otherwise exercising their privacy rights.²⁸

To prevent some of the worst abuses associated with financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The CCPA prohibits financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.²⁹ And, the AG currently has the authority under the CCPA to issue rules with respect to financial incentives.³⁰ Thus, we urge the AG to exercise its authority to prohibit the use of financial incentives in market sectors that lack competition. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates—about \$30 per month—for not leveraging U-Verse data for ad targeting.³¹ Where consumers have few choices, market forces don't impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,³² further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.³³ The AG should exercise its authority to put reasonable limits on these programs in consolidated markets.

W382-6

²⁷ Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.

²⁸ Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).

²⁹ *Id.* at § 1798.125(b)(4).

³⁰ *Id.* at § 1798.185(a)(6).

³¹ Jon Brodtkin, *AT&T To End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), <https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/>.

³² *Too Much of a Good Thing*, THE ECONOMIST (March 26, 2016), <https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing>.

³³ *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets*, Fed. Trade Comm'n (Feb. 26, 2019), <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology>.

The AG should clarify a non-exclusive list of browser privacy signals that shall be honored as a universal opt out of sale.

We appreciate that the AG has maintained the requirement that companies must honor browser privacy signals as an opt out of sale.³⁴ Forcing consumers to opt out of every company, one by one is simply not workable. However, the current rules should be adjusted to ensure that it is consumer-friendly. The AG should state that platform-level controls to limit data sharing should be interpreted as CCPA opt outs, including Do Not Track and Limit Ad Tracking. Or at the very least, the AG should clarify how platforms can certify that new or existing privacy settings should be construed as CCPA opt outs.

To encourage the development and awareness of, and compliance with, privacy settings for other platforms, we reiterate our request that the AG to issue rules governing: 1) how the developer of a platform may designate a particular privacy control to be deemed a valid request; 2) how the attorney general shall maintain and publish a comprehensive list of privacy controls to be deemed valid requests; and 3) the conditions under which business may request an exception to sell data notwithstanding a consumer’s valid request.

W382-7

Millions of consumers have signed up for Do Not Track, but there are other settings that are far less well-known, in part because they’re not associated with online use. For example, Apple, in 2013 introduced a mandatory “Limit Ad Tracking” setting for iPhone applications, and recently improved that tool to further limit the information advertisers can receive when the setting is activated.³⁵ Consumers also need global opt outs from sale when using their smart televisions and voice assistants. In order to better raise awareness of the different options on the market, to encourage the development of new tools, and to address the lack of clarity around which browser settings must be honored as opt outs, the AG should set up a system in order to make this clear for consumers and businesses.

Additionally, it would be helpful to provide guidance outside of the rule that signals such as the Global Privacy Control—a new, CR-supported effort to create a “Do Not Sell” browser signal³⁶—are likely to be considered binding in the future.

Conclusion

The proposed rules, particularly the guidance on opt-out requests, will help rein in some of the worst abuses of the opt-out process. But more needs to be done in order to ensure that the CCPA

³⁴ § 999.315(c).

³⁵ Lara O’Reilly, *Apple’s Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You*, BUS. INSIDER (Sept. 10, 2016), <http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9>.

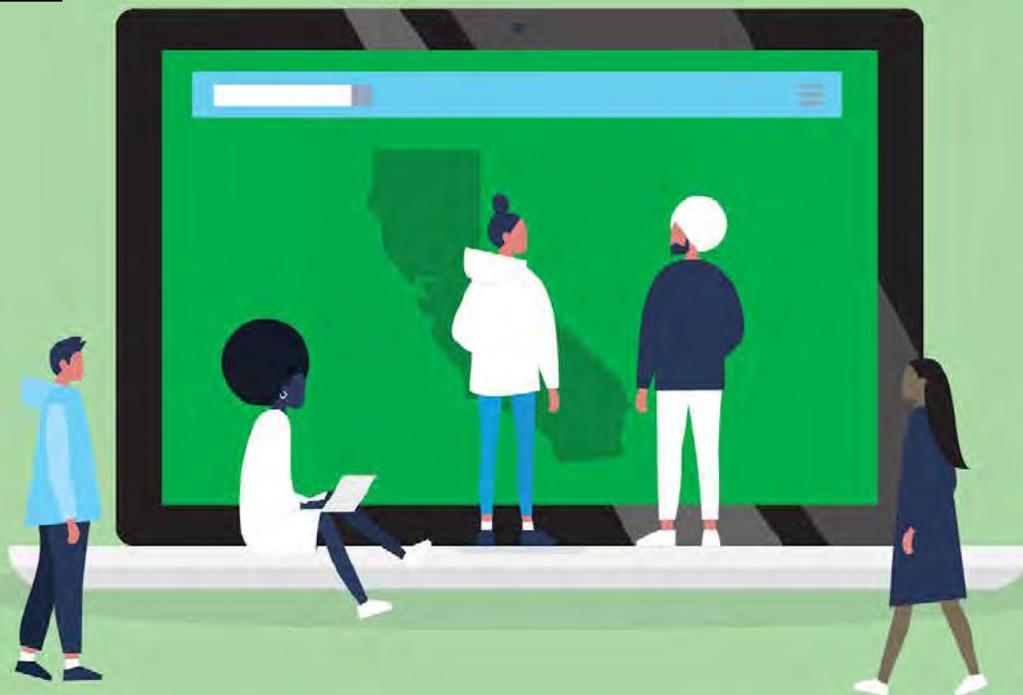
³⁶ Press release, *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights*, Global Privacy Control (Oct. 7, 2020), <https://globalprivacycontrol.org/press-release/20201007> html.

is working as intended. We look forward to working with you to ensure that consumers have the tools they need to effectively control their privacy.

Respectfully submitted,

Maureen Mahoney
Policy Analyst
Consumer Reports

The following report is in support of comments W382-1 through W382-7.



California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

MAUREEN MAHONEY

OCTOBER 1, 2020

Table of Contents

Acknowledgments	3
Executive Summary	4
Introduction	6
Companies' Responsibilities Under the CCPA	8
Methodology	10
Findings	13
Policy Recommendations	44
Conclusion	48
Appendix	49

Acknowledgments

This report is the result of a team effort. Thanks especially to Ben Moskowitz and Leah Fischman for shepherding us through this project, and to Justin Brookman, who provided invaluable assistance throughout. Devney Hamilton, Tom Smyth, and Jill Dimond at Sassafras Tech Collective deserve much of the credit for their work in devising the research study, building the testing tool, and analyzing the results. Kimberly Fountain, Alan Smith, and Daniela Nunez helped us recruit volunteers to participate in the study. Kaveh Waddell made countless contributions and Jennifer Bertsch offered crucial troubleshooting. Karen Jaffe, Camille Calman, Heath Grayson, David Friedman, and Cyrus Rassool improved the report through their review and support. Tim LaPalme and the creative team at Consumer Reports designed the report and helped us present the results more clearly. Finally, our deepest gratitude to the volunteer testers, without whom we would not have been able to conduct this study.

Executive Summary

In May and June 2020, Consumer Reports' Digital Lab conducted a mixed methods study to examine whether the new California Consumer Privacy Act (CCPA) is working for consumers. This study focused on the Do-Not-Sell (DNS) provision in the CCPA, which gives consumers the right to opt out of the sale of their personal information to third parties through a "clear and conspicuous link" on the company's homepage.¹ As part of the study, 543 California residents made DNS requests to 214 data brokers listed in the California Attorney General's data broker registry. Participants reported their experiences via survey.

Findings

- Consumers struggled to locate the required links to opt out of the sale of their information. For 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a "Do Not Sell" link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.
 - Follow-up research focused on the sites in which all three testers did not find the link revealed that at least 24 companies on the data broker registry do not have the required DNS link on their homepage.
 - All three testers were unable to find the DNS links for five additional companies, though follow-up research revealed that the companies did have DNS links on their homepages. This also raises concerns about compliance, since companies are required to post the link in a "clear and conspicuous" manner.
- Many data brokers' opt-out processes are so onerous that they have substantially impaired consumers' ability to opt out, highlighting serious flaws in the CCPA's opt-out model.
 - Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software.
 - Some data brokers asked consumers to submit information or documents that they were reluctant to provide, such as a government ID number, a photo of their government ID, or a selfie.
 - Some data brokers confused consumers by requiring them to accept cookies just to access the site.

¹ Cal. Civ. Code § 1798.135(a)(1).

- Consumers were often forced to wade through confusing and intimidating disclosures to opt out.
- Some consumers spent an hour or more on a request.
- At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.
- At least one data broker used information provided for a DNS request to add the user to a marketing list, in violation of the CCPA.
- At least one data broker required the user to set up an account to opt out, in violation of the CCPA.
- Consumers often didn't know if their opt-out request was successful. Neither the CCPA nor the CCPA regulations require companies to notify consumers when their request has been honored. About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.
- About 52% of the time, the tester was "somewhat dissatisfied" or "very dissatisfied" with the opt-out processes.
- On the other hand, some consumers reported that it was quick and easy to opt out, showing that companies can make it easier for consumers to exercise their rights under the CCPA. About 47% of the time, the tester was "somewhat satisfied" or "very satisfied" with the opt-out process.

Policy recommendations

- The Attorney General should vigorously enforce the CCPA to address noncompliance.
- To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales in one step.
- The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.
- The AG should require companies to notify consumers when their opt-out requests have been completed, so that consumers can know that their information is no longer being sold.
- The legislature or AG should clarify the CCPA's definitions of "sale" and "service provider" to more clearly cover data broker information sharing.
- Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data

minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.

Introduction

California consumers have new rights to access, delete, and stop the sale of their information under the landmark California Consumer Privacy Act, one of the first—and the most sweeping—online privacy laws in the country.² However, as the CCPA went into effect in January 2020, it was unclear whether the CCPA would be effective for consumers. Though the CCPA was signed into law in June 2018, many companies spent most of the 2019 legislative session working to weaken the CCPA.³ Early surveys suggested that some companies were dragging their feet in getting ready for the CCPA.⁴ And some companies, including some of the biggest such as Facebook and Google, declared that their data-sharing practices did not fall under the CCPA.⁵ We suspected that this disregard among the biggest and most high-profile entities would filter down to many other participants in the online data markets, and decided to further explore companies' compliance with the CCPA.

The CCPA's opt-out model is inherently flawed; it places substantial responsibility on consumers to identify the companies that collect and sell their information, and to submit requests to access it, delete it, or stop its sale. Even when companies are making a good-faith effort to comply, the process can quickly become unmanageable for consumers who want to opt out of data sale by hundreds if not thousands of different companies. Given that relatively few consumers even know about the CCPA,⁶

² Cal. Civ. Code § 1798 et seq.; Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (Jun. 28, 2018), <https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>.

³ Press Release, Consumer Reports et al., *Privacy Groups Praise CA Legislators for Upholding Privacy Law Against Industry Pressure* (Sept. 13, 2019), https://advocacy.consumerreports.org/press_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/.

⁴ *Ready or Not, Here it Comes: How Prepared Are Organizations for the California Consumer Privacy Act?* IAPP AND ONETRUST at 4 (Apr. 30, 2019), https://iapp.org/media/pdf/resource_center/IAPPOneTrustSurvey_How_prepared_for_CCPA.pdf (showing that “[M]ost organizations are more unprepared than ready to implement what has been heralded as the most comprehensive privacy law in the U.S. ever.”)

⁵ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, MEDIUM (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>

⁶ *Report: Nearly Half of U.S.-Based Employees Unfamiliar with California Consumer Privacy Act (CCPA)*, MEDIAPRO (Apr. 30, 2019), <https://www.mediapro.com/blog/2019-eye-on-privacy-report-mediapro/>.

participation is likely fairly low. Anecdotally, those that are aware of the CCPA and have tried to exercise their new privacy rights have struggled to do so.⁷ Through this study we sought to get better insight into the challenges faced by consumers trying to exercise their rights under the CCPA's opt-out model.

This study also seeks to influence the regulations implementing the CCPA, to help ensure that they are working for consumers. The CCPA tasks the California Attorney General's office with developing these regulations, which help flesh out some of the responsibilities of companies in responding to consumer requests.⁸ For example, with respect to opt outs, the regulations clarify how long the companies have to respond to opt-out requests⁹ and outline the notices that need to be provided to consumers.¹⁰ On August 14, 2020, the AG regulations went into effect.¹¹ The CCPA directs the AG to develop regulations as needed to implement the CCPA, consistent with its privacy intent,¹² and the AG has signaled that they plan to continue to consider a number of issues with respect to opt outs.¹³

The AG is also tasked with enforcing the CCPA, and this study is also intended to help point out instances of potential noncompliance. Despite efforts of industry to push back the date of enforcement,¹⁴ the AG has had the authority to begin enforcement since July 1, 2020.¹⁵ Already, the AG's staff has notified companies of potential violations of the CCPA.¹⁶

⁷ Geoffrey Fowler, *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST (Feb. 19, 2020), <https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/>.

⁸ Cal. Civ. Code § 1798.185(a).

⁹ Cal. Code Regs. tit. 11 § 999.315(e) (2020).

¹⁰ *Id.* at § 999.304-308.

¹¹ State of California Department of Justice, CCPA Regulations (last visited Aug. 15, 2020), <https://www.oag.ca.gov/privacy/ccpa/regs>.

¹² Cal. Civ. Code § 1798.185(b)(2).

¹³ Cathy Cosgrove, *Important Commentary from Calif. OAG in Proposed CCPA Regulations Package*, IAPP (Jul. 27, 2020), <https://iapp.org/news/a/important-commentary-from-calif-oag-in-proposed-ccpa-regulations-package/>.

¹⁴ See, e.g. Andrew Blustein, *Ad Industry Calls for Delayed Enforcement of CCPA*, THE DRUM (Jan. 29, 2020), <https://www.thedrum.com/news/2020/01/29/ad-industry-calls-delayed-enforcement-ccpa>; Association of National Advertisers, ANA and Others Ask for CCPA Enforcement Extension (Mar. 18, 2020), <https://www.ana.net/blogs/show/id/rr-blog-2020-03-ANA-and-Others-Asks-for-CCPA-Enforcement-Extension>.

¹⁵ Cal. Civ. Code § 1798.185(c).

¹⁶ Cosgrove, *Important Commentary*, *supra* note 13; Malia Rogers, David Stauss, *CCPA Update: AG's Office Confirms CCPA Enforcement Has Begun*, JD SUPRA (Jul. 14, 2020), <https://www.jdsupra.com/legalnews/ccpa-update-ag-s-office-confirms-ccpa-55113/>.

Our study revealed flaws in how companies are complying with CCPA and with the CCPA itself. Many companies are engaging in behavior that almost certainly violates the CCPA. But even if companies were complying completely in good faith, the CCPA makes it incredibly difficult for individuals to meaningfully exercise control over the sale of their personal information. Indeed, the conceit that consumers should have to individually opt out of data sale from each of the hundreds of companies listed on the California data broker registry—let alone the hundreds or thousands of other companies that may sell consumers' personal information—in order to protect their privacy is absurd. Over half of the survey participants expressed frustration with the opt-out process, and nearly half were not even aware if their requests were honored by the recipient. The Attorney General should aggressively enforce the current law to remediate widespread noncompliant behavior, but it is incumbent upon the legislature to upgrade the CCPA framework to protect privacy by default without relying upon overburdened consumers to understand complex data flows and navigate heterogenous privacy controls.

Companies' responsibilities under the CCPA

Under the CCPA, companies that sell personal information (PI) to third parties must honor consumers' requests to opt out of the sale of their PI.¹⁷ The CCPA has a broad definition of personal information, which includes any data that is reasonably capable of being associated with an individual or household—everything from Social Security numbers, to biometric information, or even browsing history. This also covers browsing history or data on a shared computer (in other words, not data that can be exclusively tied to a single individual)¹⁸—further highlighting that opt outs need not be verified to a particular individual. The CCPA's definition of sale covers any transfer of data for valuable consideration,¹⁹ intended to capture data that is shared with third parties for behavioral advertising purposes.²⁰

¹⁷ Cal. Civ. Code § 1798.120(a).

¹⁸ *Id.* at § 1798.140(o)(1).

¹⁹ *Id.* at § 1798.140(t)(1).

²⁰ California Senate Judiciary Committee, SB 753 Bill Analysis at 10 (Apr. 22, 2019), https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200SB753. The analysis excerpts a letter from the sponsors of AB 375, Californians for Consumer Privacy, opposing SB 753, legislation proposed in 2019 that would explicitly exempt cross-context targeted advertising from the CCPA: "SB 753 proposes to amend the definition of "sell" in Civil Code Section 1798.140 in a manner that will break down th[is] silo effect As a result, even if a consumer opts-out of the sale of their data, this proposal would allow an advertiser to combine, share and proliferate data throughout the advertising

The CCPA places certain responsibilities on these companies to facilitate the opt outs. They are required to provide a “clear and conspicuous link” on their homepage so that consumers can exercise their opt-out rights.²¹ The CCPA pointedly creates a separate process for exercising opt-out rights than it does for submitting access and deletion requests—the latter requires verification to ensure that the data that is being accessed or deleted belongs to the correct person.²² In contrast, for opt outs, verification is not required.²³ Importantly, companies may not use the information provided by the opting out consumer for any other purpose.²⁴ The CCPA also directs the AG to design and implement a “Do Not Sell” button to make it easier for consumers to opt out.²⁵

The AG’s regulations outline additional requirements. Companies must post a prominent link labeled “Do Not Sell My Personal Information,” which must lead the consumer to the required interactive form to opt out.²⁶ (The AG declined to finalize a design to serve as an opt-out button.)²⁷ CCPA regulations clarify that “A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request[,]” and the company, if it declines a request for that reason, is required to notify the consumer and provide an explanation.²⁸ Companies must honor consumers’ requests to opt out within 15 business days²⁹ (in contrast to 45 days for deletion and access requests).³⁰

economy. The proposed language will essentially eliminate the silo effect that would occur pursuant to the CCPA, which allows for targeted advertising but prevents the proliferation of a consumer’s data throughout the economy.”

²¹ Cal. Civ. Code § 1798.135(a)(1).

²² *Id.* at § 1798.140(y).

²³ *Id.* at § 1798.135.

²⁴ *Id.* at § 1798.135(a)(6).

²⁵ *Id.* at § 1798.185(a)(4)(C).

²⁶ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

²⁷ State of California Department of Justice, Final Statement of Reasons at 15 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf> [hereinafter FSOR].

²⁸ *Id.* at § 999.315(g).

²⁹ *Id.* at § 999.315(e).

³⁰ Cal. Civ. Code §1798.130(a)(2).

Methodology

In this section, we describe our sample, the research exercise, survey, and method of analysis.

Selecting Companies to Study

To select the companies to study, we used the new California data broker registry,³¹ which lists companies that sell California consumers' personal information to third parties, but do not have a direct relationship with the consumer.³² Reining in data brokers—which profit from consumers' information but typically do not have a direct relationship with them—was a primary purpose of the CCPA. Through the opt out of sale, the authors of the CCPA sought to dry up the pool of customer information available on the open market, disincentivize data purchases, and make data brokering a less attractive business model.³³

The data broker registry was created in order to help consumers exercise their rights under the CCPA with respect to these companies. Companies that sell the personal information of California consumers but don't have a relationship with the consumer are required to register with the California Attorney General each year.³⁴ The AG maintains the site, which includes the name of the company, a description, and a link to the company's website, where the consumer can exercise their CCPA rights.³⁵ The data broker registry is particularly important because many consumers do not even know which data brokers are collecting their data, or how to contact them. Without the data broker registry, exercising CCPA rights with respect to these companies would be near impossible.

For many consumers, data brokers exemplify some of the worst aspects of the ad-supported internet model, giving participants in the study a strong incentive to opt out of the sale of their information. Nearly everything a consumer does in the online or even physical world can be collected, processed, and sold by data brokers. This could

³¹ State of California Department of Justice, Data Broker Registry (last visited August 10, 2020), <https://oag.ca.gov/data-brokers> [hereinafter DATA BROKER REGISTRY].

³² Cal. Civ. Code § 1798.99.80(d).

³³ Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

³⁴ DATA BROKER REGISTRY, *supra* note 31.

³⁵ *Id.*

include location data picked up from apps, purchase history, browsing history—all combined to better understand and predict consumer behavior, and to guide future purchases. Data brokers can purchase information from a variety of sources, both online and offline, including court records and other public documents. The inferences drawn can be startlingly detailed and reveal more about a consumer than they might realize. Consumers can be segmented by race, income, age, or other factors.³⁶ The information collected can even provide insight whether a consumer is subject to certain diseases, such as diabetes, or other insights into health status.³⁷ All of this data might be used for marketing, or it could be used to assess consumers' eligibility for certain opportunities, either due to loopholes in consumer protection statutes such as the Fair Credit Reporting Act, or because of a lack of transparency and enforcement.³⁸

Sampling

We randomly sampled from all of the 234 brokers in California's data broker registry as of April 2020. In the final analysis, we included three sample requests for each of 214 brokers, totaling 642 DNS requests made by 403 different participants. Though we did not have enough testers to ensure that every company on the data broker registry received three tests, a sample of 214 of 234 companies in the database is more than sufficient to represent the different types of processes for all companies. In our initial investigation into DNS requests, in which we submitted our own opt-out requests, we found that three requests were generally enough to uncover the different processes and pitfalls for each company. However, in order to analyze and generalize success rates of DNS requests depending on different processes, a follow-up study should be conducted toward this end. In cases in which testers submitted more than three sample requests for a company, we randomly selected three to analyze.

Participants were not representative of the general population of California. As this initial study was designed to understand the landscape of different data brokers and their DNS request processes, we decided to use a convenience sample. Participants were

³⁶ *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N at 24 (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

³⁷ *Id.* at 25.

³⁸ *Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. at 26 (Mar. 2014), <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>; *Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>.

recruited through CR's existing membership base, promotion by partner organizations, and through social media outreach. Participation was limited to California residents. Therefore, participants were likely better informed about the CCPA and digital privacy rights than the general population. The study was conducted in English, excluding those not fluent in English. Participation in the study was not compensated.

Research Exercise

In the study exercise, participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that data broker. Participants could, and many did, test more than one data broker. On average, participants performed 1.8 test requests. For each request, the participant was given a link to the data broker's website and its email address. They were instructed to look for a "Do Not Sell My Personal Info" (or similar) link on the broker's site and to follow the instructions they found there, or to send an email to the email address listed in the data broker registration if they did not find the link. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker. (See Appendix, Section A for a diagram of the participant experience of the exercise).

Survey Design

The survey aimed to capture a description of a participant's experience in making a DNS request. We approached the design of this study as exploratory to understand the DNS process and as a result, asked mixed qualitative and quantitative questions. The survey branched to ask relevant questions based on what the participant had reported thus far. These questions involved mostly optional multi-select questions, with some open-ended questions. Because the survey included optional questions, not all samples have answers to every question. We omitted from the analysis samples in which there was not enough applicable information for the analysis question. Participants were encouraged to use optional "other" choices with open-ended text. We also offered participants the ability to send in explanatory screenshots. Where participants flagged particularly egregious behaviors, we followed up by having a contractor collect screenshots, or we followed up ourselves to collect screenshots.

Data Analysis

We used both quantitative and qualitative methods for analysis. To answer the questions of time spent and ability to find the DNS request link, we aggregated the responses. To understand the result of request processes, we relied on answers to both open-ended text questions and multi-select questions related to status in order to code and tally the results.

For open response text, we used a qualitative thematic analysis approach where we read the text and coded inductively for themes.

Limitations

This was an exploratory study designed to uncover different DNS processes. As such, our results are not experimental and cannot conclusively establish the efficacy of these DNS processes. Some questions in the survey were meant to capture the participants' experiences, such as "Did the [broker] confirm that they are not selling your data?" For example, a confirmation email could have been sent to the consumer's junk mail folder—so the consumer may not have been aware of the confirmation, even if the company had sent one. Also, consumers may not have understood brokers' privacy interfaces, and conflated DNS requests with other rights; for example, some consumers may have submitted access or deletion requests when they meant to submit opt-out requests. That said, given that the CCPA is designed to protect consumers, consumers' experiences have value in evaluating the CCPA. In addition, because of our convenience sample, it is likely that the broader population may generally drop off from these processes earlier (or not engage at all) due to constraints such as time or lack of technology skill.

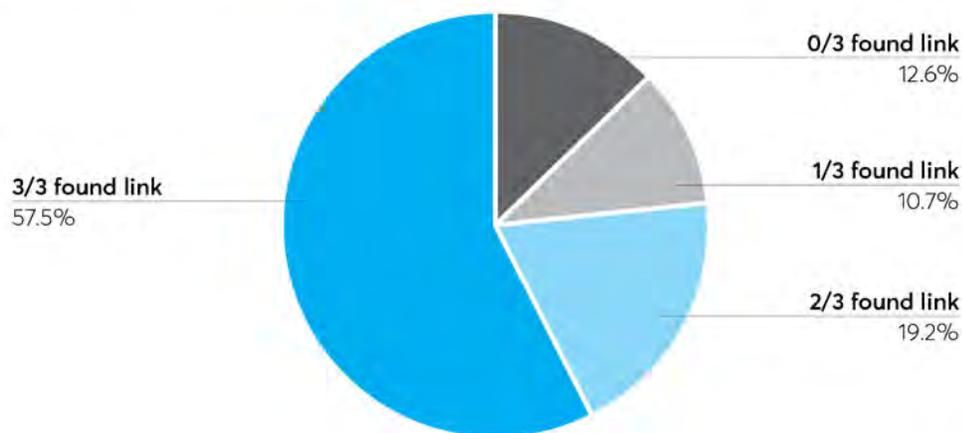
Findings

CCPA opt outs should be simple, quick, and easy. However, we found that many companies failed to meet straightforward guidelines—posing significant challenges to consumers seeking to opt out of the sale of their information. Below, we explore the challenges consumers faced in opting out of the sale of their information from data brokers.

For 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a “Do Not Sell” link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.

Consumers often found it difficult to opt out of the sale of their information, in large part because opt-out links either weren't visible on the homepage or weren't there at all. Nearly half the time, at least one of three of our testers failed to find the link, even though they were expressly directed to look for it. This suggests that either the link wasn't included on the homepage, or that it was not listed in a “clear and conspicuous” manner, both of which are CCPA requirements.

Brokers by number of testers who found DNS link



Companies on the California data broker registry by definition sell customer PI to third parties and should have a Do Not Sell link on their homepage in order to comply with the CCPA. Under California law, every data broker is required to register with the California Attorney General so that their contact information can be placed on the registry.³⁹ A data broker is defined as a “business that knowingly collects *and sells* to third parties the personal information of a consumer with whom the business does not have a direct relationship.”⁴⁰ [emphasis added] The definitions of “sell,” “third parties,”

³⁹ Cal. Civ. Code §1798.99.82.

⁴⁰ *Id.* at § 1798.99.80(d).

and “personal information” all mirror those of the CCPA, which helps to ensure that the registry effectively aids consumers in exercising their CCPA rights with respect to these entities.⁴¹

While it is true that some data brokers may enjoy certain exemptions from AB 1202, companies selling customer information still are obligated to put up Do Not Sell links. In response to requests to the AG during the rulemaking process to “Amend [the CCPA rules] to explain that businesses must provide notice of consumer rights under the CCPA only where such consumer rights may be exercised with respect to personal information held by such business. Consumer confusion could result from explanation of a certain right under the CCPA when the business is not required to honor that right because of one or more exemptions[,]” the AG responded that “CCPA-mandated disclosures are required even if the business is not required to comply with the consumers’ exercise of their rights.”⁴²

The homepage means the first, or landing, page of a website. It is not sufficient to place a link to a privacy policy on the first page, that leads to the DNS link—the link on the homepage must be labeled “Do Not Sell My Personal Information.”⁴³ The CCPA clarifies that “homepage” indeed means “the introductory page of an internet website and any internet web page where personal information is collected.”⁴⁴ The AG further explains that a link to a privacy policy is not sufficient to constitute a Do Not Sell link: “The CCPA requires that consumers be given a notice at collection, notice of right to opt out, and notice of financial incentive. These requirements are separate and apart from the CCPA’s requirements for the disclosures in a privacy policy.”⁴⁵

The CCPA does note that a company need not include “the required links and text on the homepage that the business makes available to the public generally[,]” if it establishes “a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for

⁴¹ *Id.* at § 1798.99.80(e)-(g).

⁴² State of California Department of Justice, Final Statement of Reasons, Appendix A, Response #264 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf> [hereinafter “FSOR Appendix”].

⁴³ Cal. Civ. Code § 1798.135(a)(1).

⁴⁴ *Id.* at § 1798.140(l).

⁴⁵ FSOR Appendix, *supra* note 42, Response #105.

California consumers and not the homepage made available to the public generally.”⁴⁶ We limited our outreach to participants who had previously told us they were California residents, though we cannot say for sure that they were in California at the time they completed our survey. Occasionally California employees supplemented survey responses by capturing additional screenshots, sometimes from within California, sometimes without. Technically, the CCPA gives rights to Californians even when they are not physically present within the state, though it is possible that data brokers treat users differently based on approximate geolocation derived from their IP address.⁴⁷

If testers are unable to find a DNS link on the homepage even if it is there, that suggests that it may not be placed in a “clear and conspicuous” manner, as required by the CCPA. If testers that have been provided instructions and are looking for an opt-out link in order to complete a survey are unable to find a link, it is less likely that the average consumer, who may not even know about the CCPA, would find it.

Testers that did not find an opt-out link but continued with the opt-out process anyway often faced serious challenges in exercising their opt-out rights. We instructed these testers to email the data broker to proceed with the opt-out request. This considerably slowed down the opt-out process, as a consumer had to wait for a representative to respond in order to proceed. And often, the agent provided confusing instructions or was otherwise unable to help the consumer with the opt-out request. For example, we received multiple complaints about Infinite Media. Infinite Media did not have a “Do Not Sell” link on its homepage (see Appendix, Section B for a screenshot). Further, its representative puzzled testers by responding to their opt-out emails with confusing questions—such as whether they had received any marketing communications from the company—in order to proceed with the opt out.

I am with Infinite Media/ Mailinglists.com and have been forwarded your request below. We are a list brokerage company and do not compile any data. We do purchase consumer data on behalf of some of our clients and we do work with a large business compiler and purchase data from them as well. Can you tell me if you received something to your home or business address? If home address I will need your full address info. If business, then please send your company name and address. Also do you work from home? Lastly who was it that you received the mail piece, telemarketing call or email from? I need to know the

⁴⁶ Cal. Civ. Code § 1798.135(b).

⁴⁷ Cal. Civ. Code § 1798.140(g).

name of the company that contacted you so I can track back where the data came from and contact the appropriate list company and have you removed from their data file so they don't resell your name any longer.

Given the number of unsolicited communications that consumers receive, it was difficult for the testers to answer and frustrated their efforts to opt out. One consumer reached out to us after receiving the message: "I don't know how to reply - since I have not received any marketing item from them, ca[n]t give them the name of outfit/person they're asking about. Our landline does get an annoying amount of robocalls and telemarketing calls but I can't tell who/what they're from...."

The agent's confusing response itself is a potential CCPA violation, as the CCPA requires companies to "[e]nsure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 [regarding the right to opt out] and this section and how to direct consumers to exercise their rights under those sections."⁴⁸ Instead of directing consumers to the interactive form to opt out, the agent confused and frustrated consumers seeking to exercise their CCPA opt-out rights by asking them questions that they could not answer.

At least 24 companies on the data broker registry do not have a DNS link anywhere on their homepages.

Follow-up research on the sites in which all three testers did not find the link revealed that at least 24 companies do not have the required DNS link on their homepage (see Appendix, Section B for screenshots).⁴⁹ For example, some companies provide information about CCPA opt-out rights within its privacy policy or other document, but offer no indication of those rights on the homepage. Since consumers typically don't read privacy policies,⁵⁰ this means that unless a consumer is familiar with the CCPA or

⁴⁸ Cal. Civ. Code § 1798.135(a)(3).

⁴⁹ These companies are: Admarketplace.com, Big Brook Media, Inc., Blue Hill Marketing Solutions, Comscore, Inc., Electronic Voice Services, Inc., Enformion, Exponential Interactive, Gale, GrayHair Software, LLC, Infinite Media Concepts Inc, JZ Marketing, Inc., LeadsMarket.com LLC, Lender Feed LC, On Hold-America, Inc. DBA KYC Data, Outbrain, PacificEast Research Inc., Paynet, Inc., PossibleNow Data Services, Inc, RealSource Inc., Social Catfish, Spectrum Mailing Lists, SRAX, Inc., USADATA, Inc., and zeotap GmbH.

⁵⁰ Brooke Axier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RESEARCH CTR. (Nov. 15, 2019),

is specifically looking for a way to opt out, they likely won't be able to take advantage of the DNS right.

For example, the data broker Outbrain doesn't have a "Do Not Sell My Personal Information" link on its homepage. The consumer can click on the "Privacy Policy" link at the bottom of the page, which sends the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer can cut out several steps by clicking on "Interest-Based Ads" on the homepage.) If a consumer would like to opt out on their phone, they would have to go through another process. And if the consumer clears their cookies, they would need to opt out again. As one consumer told us, "It was not simple and required reading the 'fine print.'" Below, we show the opt-out process through screenshots (See pages 20-21):

STEP 1 The "Privacy Policy" link takes the consumer to the "Privacy Center." Consumers can click on panel 6, "California Privacy Rights," **STEP 2.**

Clicking on "California Privacy Rights" opens up a text box **STEP 3**, that includes a bullet on the "Right to opt-out of the 'sale' of your Personal Information." That section includes a very small hyperlink to "opt out of personalised recommendations."

Clicking on that link takes the consumer to another to a page titled "Your Outbrain Interest Profile," **STEP 4.** (The consumer can also reach this page by clicking on "Interest-Based Ads" on the homepage.)

The consumer can then click on "View My Profile," which takes them to a new page that provides a breakdown of interest categories. In the upper right-hand corner, there is a small, gray-on-black link to "Opt Out," **STEP 5.**

This finally takes the consumer to a page where they can move a toggle to "opt out" of interest-based advertising, **STEP 6**, though it is unclear whether turning off personalized recommendations is the same as opting out of the sale of your data under the CCPA. One tester remarked on the confusion, "There were many links embedded in the Outbrain Privacy Center page. I had to expand each section and read the text and review the links to determine if they were the one I wanted. I am not sure I selected "DO not Sell" but I did opt out of personalized advertising."

<https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/> (Showing that only 9% of adults read the privacy policy before accepting the terms and conditions, and 36% never do.).

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

Outbrain Advertisers Publishers About Us Help Center Blog Careers Contact Us Register

The Open Web's
Discovery & Native Advertising Feed

Advertise with Us Publishers, Let's Talk

Privacy Policy

STEP 1

4. Children
5. European Territory Citizens
6. California Privacy Rights
7. "Do Not Track" Disclosure
8. How This Privacy Policy May Change

STEP 2

- ◆ Right to opt-out of the "sale" of your Personal Information. We do not sell your Personal Information in the conventional sense (i.e., for money). However, like many companies, we use services that help deliver interest-based ads to you. California law classifies our use of these services as a "sale" of your Personal Information to the companies that provide the services. This is because we allow them to collect information from our website users (e.g., online identifiers and browsing activity) so they can help serve ads more likely to interest you.] To opt-out of this "sale," click on **this link** which will take you to our Interest Profile where you can opt out of personalised recommendations.

STEP 3

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

STEP 4

STEP 5

STEP 6

Our promise to you is transparency and choice.

Select your recommendation settings below:

- Personalized Interest Recommendations
- Non-Personalized Recommendations (Opt Out)

Mobile Application Opt-Out

Simply update your mobile device settings to opt-out of Outbrain recommendations on your mobile applications.

iOS Devices: Settings > Privacy > Advertising > Limit Ad Tracking

Android Devices: Google Settings App > Ads > Opt Out of Interest-based Advertising

Even those steps don't opt consumers out for all devices. There are separate instructions for opting out on a mobile device, and for bulk opting out of ad targeting through a voluntary industry rubric (though again, it isn't clear if this is the same as stopping sale under the CCPA).

Instead of leaving consumers to navigate through multiple steps to opt out, Outbrain should have included a link that says "Do Not Sell My Personal Information" on the homepage, and then immediately taken the consumer to a page with the toggle to opt out. The AG's regulations require companies to provide "two or more designated methods for submitting requests to opt out, including an *interactive form* accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application."⁵¹ (emphasis added). This suggests that the opt out is intended to involve nothing more than filling out a short form, one that is quickly and easily accessed from the homepage.

For an additional five companies, all three testers were unable to find the DNS link, suggesting that they may not be listed in a "clear and conspicuous" manner as required by the CCPA.

All three testers were unable to find the DNS link for an additional five companies (see Appendix, Section C for screenshots).⁵² For example, all three testers failed to find the Do Not Sell link for the data broker Freckle I.O.T. Ltd./PlacelQ. First, the website <https://freckleiot.com/>, which is listed on the data broker registry, automatically redirects to <https://www.placeiq.com/>, where consumers are confronted with a dark pattern banner at the bottom of the screen that only offers the option to "Allow Cookies" (the banner also states that "scrolling the page" or "continuing to browse otherwise" constitutes consent to place cookies on the user's device.) If the user does not click "Allow," the banner stays up, and it obscures the "CCPA & Do Not Sell" link (for more on mandating cookie acceptance as a condition of opting out, see *infra*, p. 30).

⁵¹ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

⁵² These companies are: AcademixDirect, Inc., Fifty Technology Ltd, Freckle I.O.T. Ltd./PlacelQ, Marketing Information Specialists, Inc., and Media Source Solutions. Two of the companies in which all three testers could not find the DNS link did not appear to have a functioning website at all: Elmira Industries, Inc. and Email Marketing Services, Inc.

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

The image shows a screenshot of the PlaceIQ website with annotations for two steps in the cookie consent process. **STEP 1** highlights a dark banner at the bottom of the page with a white 'Allow cookies' button. **STEP 2** highlights a dark footer area with a 'Consumer Options' menu, where 'Privacy Policy' and 'CCPA & Do Not Sell' are listed. A white arrow points from Step 1 to Step 2.

PlaceIQ

Solutions ▾ News & Resources ▾ About Us ▾ [CONTACT US](#)

Check out PlaceIQ's latest COVID-19 research and analysis, and sign up for our weekly newsletter! [LEARN MORE](#)

Ten years ago, PlaceIQ invented location intelligence for the marketing and media space. Today, we are the leading data and technology company that helps businesses leverage insights to connect with their customers.

[PlaceIQ Data Cloud](#) [experian.](#) [comscore](#) [MARKETING EVOLUTION](#)

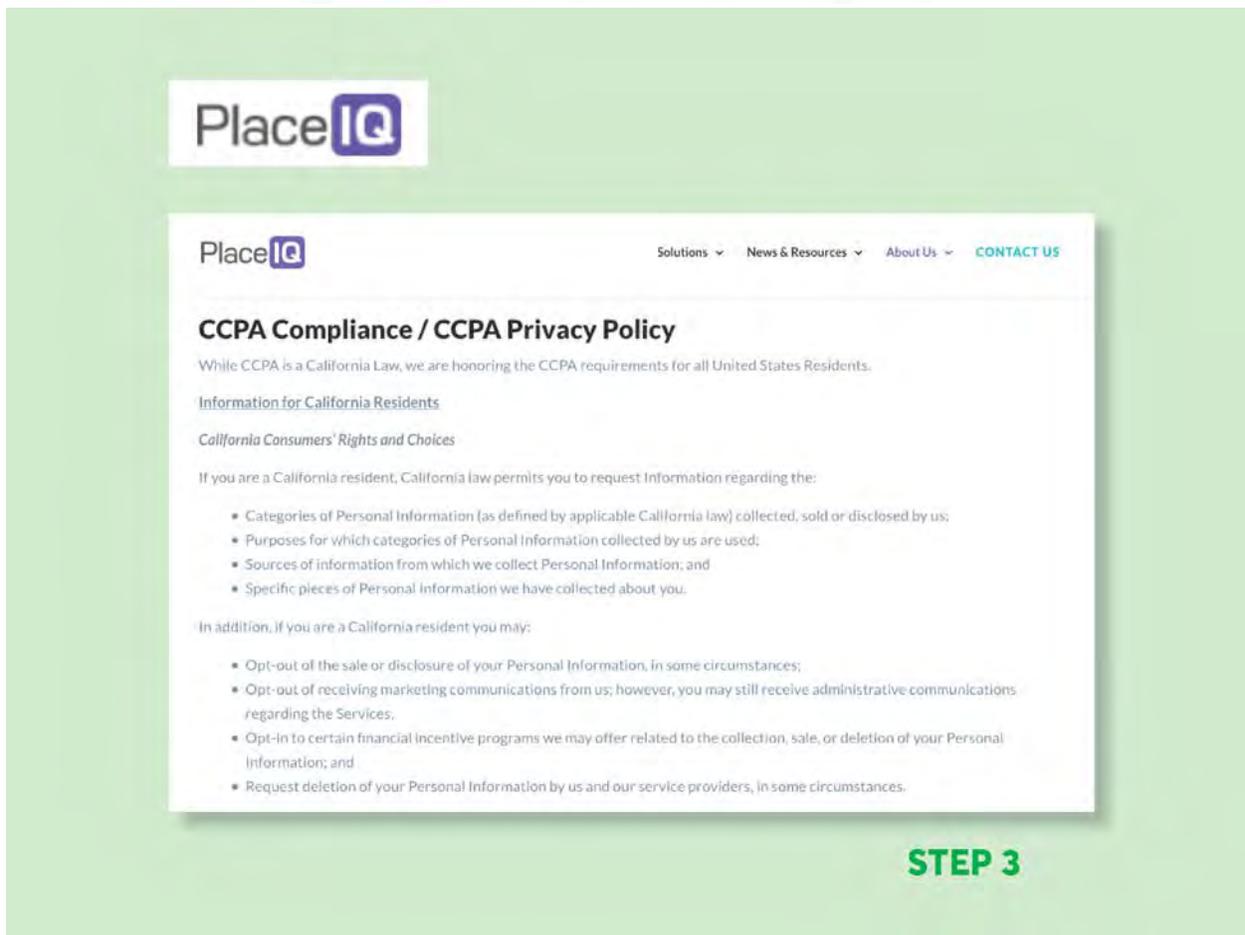
We use cookies to ensure that we give you the best experience on our website. If you want to know more or withdraw your consent to all or some of the cookies, please refer to the [cookie policy](#). By closing this banner, scrolling this page, clicking a link or continuing to browse otherwise, you agree to the use of cookies. [Allow cookies](#)

STEP 1

Allow cookies

STEP 2

Consumer Options:
Privacy Policy,
CCPA & Do Not Sell



After clicking “Allow Cookies,” revealing the full homepage, then, the user must scroll all the way down to the bottom of the homepage to get to the CCPA & Do Not Sell link (also note that the link is not labeled “Do Not Sell My Personal Information” as required by the CCPA).

Since users must accept cookies to remove the pop up and reveal the link, and the link was buried at the very bottom of the page, it is not surprising that none of the consumers testing the site were able to find the opt-out link, even though they were looking for it. This shows how confusing user interfaces can interfere with consumers’ efforts to exercise their privacy preferences, and how important it is for companies to follow CCPA guidance with respect to “clear and conspicuous” links. Without an effective mechanism to opt out, consumers are unable to take advantage of their rights under the law.

Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software, raising serious questions about the workability of the CCPA for consumers.

While companies might need to collect some information from consumers in order to identify consumer records—for example, data brokers typically sell records by email⁵³—some companies asked for information that was difficult to obtain, or required consumers to undergo onerous processes in order to opt out. There were a variety of formats for making DNS requests such as instructions to download a third-party app, instructions to send an email, or no instruction or clearly visible opt-out link at all (we instructed our participants to send an email to the email address in the registry if they could not find the opt-out link).

The most common type of DNS process involved filling out a form with basic contact information such as name, email, address, and phone number. However, several companies, such as those tracking location data, asked consumers to provide an advertising ID and download a third-party app to obtain it. This was confusing and labor intensive for many testers.

Companies that defaulted to pushing consumers to install an app to obtain the ID discouraged some consumers from opting out—downloading a separate app to their phone was a step too far. One tester of data broker Freckle I.O.T./PlacelQ reported, “Too technically challenging and installing an app on your phone shouldn't be required.” The consumer further notes that the Freckle I.O.T./PlacelQ opt-out process would be impossible for consumers without a mobile phone. “The process also could not be completed on a computer, so anyone without a smartphone would not be able to complete the request this way.” In nearly half (8 out of 20) of cases, consumers declined to provide an advertising or customer ID.

Other consumers found themselves unable to submit opt-out requests because the company required an IP address. For example, four testers reported that they could not complete their request to Megaphone LLC because they were asked to provide their IP address. In this case, it was likely that testers declined to proceed further because they could not figure out how to obtain their IP address. The screenshot on page 25 shows that Megaphone’s opt-out form includes a required question, “What is your IP address?”

⁵³ For example, TowerData claims that clients can obtain “data on 80% of U.S. email addresses.” TowerData (last visited Sept. 13, 2020), <http://intelligence.towerdata.com/>.

The image shows a sequence of two steps for handling a CCPA request on the Megaphone website.
STEP 1: A screenshot of the Megaphone homepage with a cookie consent banner at the bottom. The banner contains the text: "Do not sell my personal information" (highlighted with a green box), "By using this site, you agree to the use of cookies by Megaphone and our partners to provide the best experience, analyze site use and deliver advertising. [Privacy Policy](#)" and a "Close" button. Below the banner is a button labeled "Do not sell my personal information".
STEP 2: A screenshot of the "CCPA Request" form. The form title is "CCPA Request" and includes a sub-header: "California residents may use this form to submit a request to opt out of the 'sale' of their personal information to third parties." Below this is a paragraph: "The only personal information that Megaphone collects is a user's IP address and user agent, which is information about the user's device, browser, and platform of origin. We require California residents to submit their IP address and the platform from which they download podcasts because, without that information, we have no way to act on their requests." The form contains the following fields: "Name", "Email address", "What is your IP address?", and "What is your user agent?" (a dropdown menu with "-Select-" selected). At the bottom, there is a checkbox for "I'm not a robot" next to a CAPTCHA logo, and a "SUBMIT" button.

Some data brokers asked consumers to submit information that they were reluctant to provide, such as a photo of their government ID.

Some companies asked consumers to verify their identities or residence, for example by providing their government ID number, an image of their government ID, or a “selfie.” Testers reported that a few asked knowledge-based authentication questions, such as previous addresses or a home where someone has made a payment.

The histogram on page 27 shows the relative frequency of types of information testers were asked for and steps they were asked to take as part of their DNS request.⁵⁴

⁵⁴ All requests are combined in this analysis (rather than broken down by broker), reflecting the overall experience of making DNS requests under the CCPA. For reporting what is asked of testers in the process, we used the answers to multi-select questions about what information testers were asked for and/or refrained from providing, and multi-select questions about actions they were asked to take and/or refrained from taking. As some of the action options were redundant of the information options, we combined a non-repeat subset of the action options with the information options. We also used text answers in these parts of the survey in qualitative analysis about the variety of DNS processes.

DNS Request Processes



A company needs some personal information in order to process a “Do Not Sell” request—if a data broker sells records linked to email addresses, it needs to know the email address about which it is no longer allowed to sell information. Nevertheless,

companies are not allowed to mandate identity verification to process a DNS request under CCPA, and requesting sensitive information provided friction and led many consumers to abandon their efforts to opt out. See, for example, the Melissa Corporation, which requested consumers to provide “verification of California residency and consumer’s identity.”

melissa

melissa

California Consumer Privacy Act Notice (Show Details...)

Right to Know

Right to Opt-Out of Sale of Personal Information

Right to Delete

Please provide the information that you want to inquire.

First Name: Last name:

Phone: Mobile Phone:

Email:

Address:

Address2:

City: State: CA ▾

ZIP/Postal Code:

*Attach verification of California residency and consumer's identity (Supported files: .pdf, .jpg, .jpeg, .gif, .bmp, .png, .tif)

Choose File No file chosen

Choose File No file chosen

Choose File No file chosen

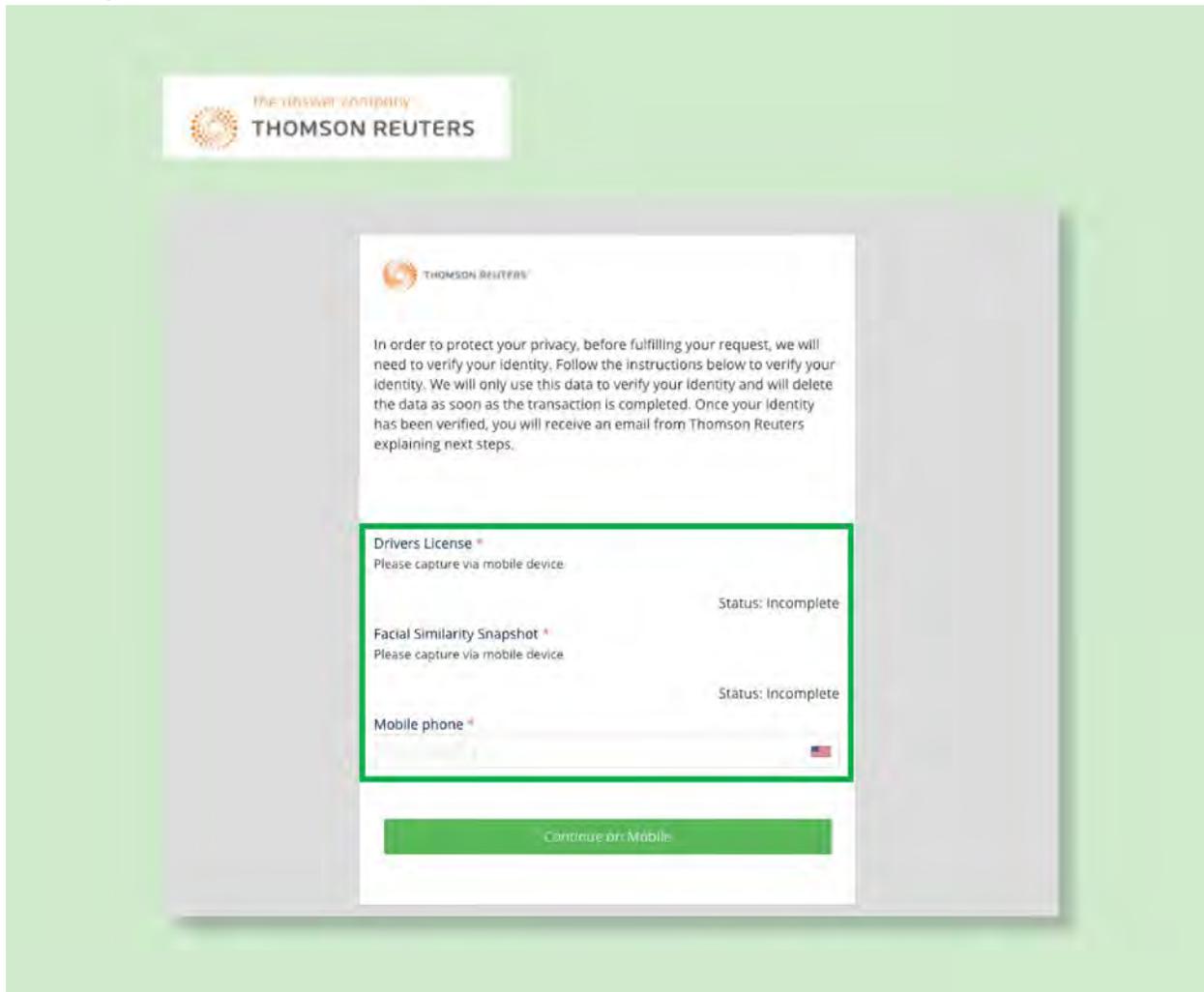
Submit

The CCPA only covers California consumers,⁵⁵ and the statute and implementing regulations are ambiguous on how companies may require consumers to prove they are

⁵⁵ Cal. Civ. Code § 1798.140(g).

covered by the law. However, asking for proof of residence added difficulty to the opt-out process, especially as other companies achieved this objective by requesting the consumer's name, address, and email.

West Publishing Corporation, part of Thomson Reuters, also asked consumers to submit to identity verification to complete the opt-out process. As shown in the screenshot below, the site requires consumers to submit a photo of their government ID and a selfie, as well as their phone number. Once the phone number is submitted, the site sends a text to help facilitate the capture of these documents through the user's mobile phone.



While these requests might be appropriate in the case of an access or deletion request, where identity verification is important to make sure that data is not being accessed or

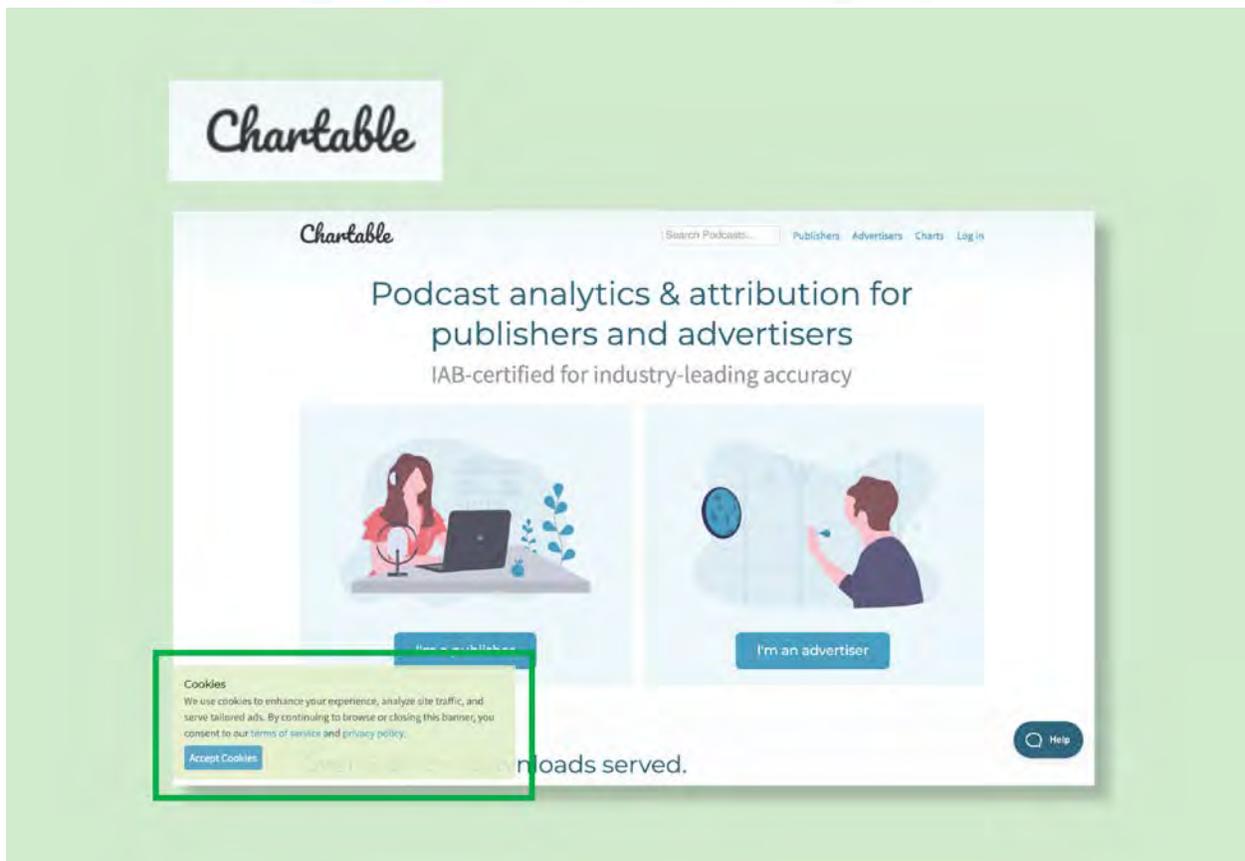
deleted without the consumer's consent, in the case of an opt out, it frustrates consumers' objectives to stop the sale of their personal information and does not provide additional privacy protection.

Some data brokers led consumers to abandon opt outs by forcing them to accept cookies.

As the CCPA went into effect in January 2020, some California consumers noticed that when they visited websites, they were asked to opt in to the use of cookies—and expressed confusion about what they were being asked to do. These notices have been common in Europe in response to the e-Privacy Directive, and more recently the Global Data Protection Regulation, though privacy advocates have been deeply critical of the practice: companies often use dubious dark patterns to nudge users to click “OK,” providing the veneer, but not the reality of, knowing consent.⁵⁶ The expansion of cookie banners in California was borne out in our study. Sixty-six of the 214 brokers had at least one consumer report a request or mandate to accept cookies as part of the DNS process. In some cases, for example if a company only tracks online using cookies, it may be reasonable for a site to set a non-unique opt-out cookie to allow the opt out to persist across multiple sessions. But the examples we saw were confusing to consumers, and did not clearly convey that a cookie was going to be placed for the limited purpose of enabling the opt out of cross-site data selling. And, as previously noted, sometimes the cookie consent banners obscured links to opt-out processes on a company's home page (see discussion of Freckle I.O.T./PlacelQ's interface, *supra* p. 21-22, and *infra* p. 31).

When visiting the website of the data broker Chartable to opt out of the sale of information, visitors are required to accept cookies. Chartable explains that the cookies are used to “serve tailored ads.” The only option is to “Accept Cookies,” and it asserts that by browsing the site users are agreeing to its terms of service and privacy policy.

⁵⁶ *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent*, PRIVACY INTERNATIONAL (last visited Aug. 28, 2020), <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>.



For nine brokers, at least one tester reported refraining from accepting cookies as part of the process. In five of these cases, testers reported that they stopped their request because they felt uncomfortable or did not understand next steps. For example, a Freckle I.O.T./PlacelQ tester described how accepting cookies was implicitly required for making a DNS request:

Their text-box asking to Allow Cookies covers the bottom 20% of the screen and won't go away unless, I assume, you tick the box to Allow. Therefore, I cannot see all my options. Also, I am accessing their site on a PC and they want me to download an app to my phone. Very difficult or impossible to see how to stop them from selling my data.

Another tester reported that the company they tested, Deloitte Consulting, had "two request types—'Cookie Based' and 'Non-Cookie Based'" and that they were "skeptical that most people will be able to decode the techno-babble description of each type."

Consumers were often forced to wade through confusing and intimidating disclosures to opt out.

While our survey did not include direct questions about communications with data brokers, in some cases consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, “There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart.” Another said of Oracle America, “The directions for opting out were in the middle of a wordy document written in small, tight font.” Another found the legal language used by Adrea Rubin Marketing intimidating: “they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury.”

Another data broker, ACBJ, placed a “Your California Privacy Rights” link at the bottom of their homepage (rather than a “Do Not Sell My Personal Information” link), which led to their privacy and cookie policy.⁵⁷ Once on the policy page, the consumer is forced to search in their browser for the phrase “Do Not Sell My Personal Information” or scroll and scan ten sections of the privacy policy to find the paragraph with a “Do Not Sell My Personal Information” link, or follow two additional links to navigate from the privacy policy table of contents to the “Do Not Sell My Personal Information” link. Upon clicking the “Do Not Sell My Personal Information” link, the consumer is shown a pop-up with a page of additional legal information, and then has to scroll down to a toggle that finally allows them to request their data not be sold.

Some consumers spent nearly an hour, if not more, to complete a request.

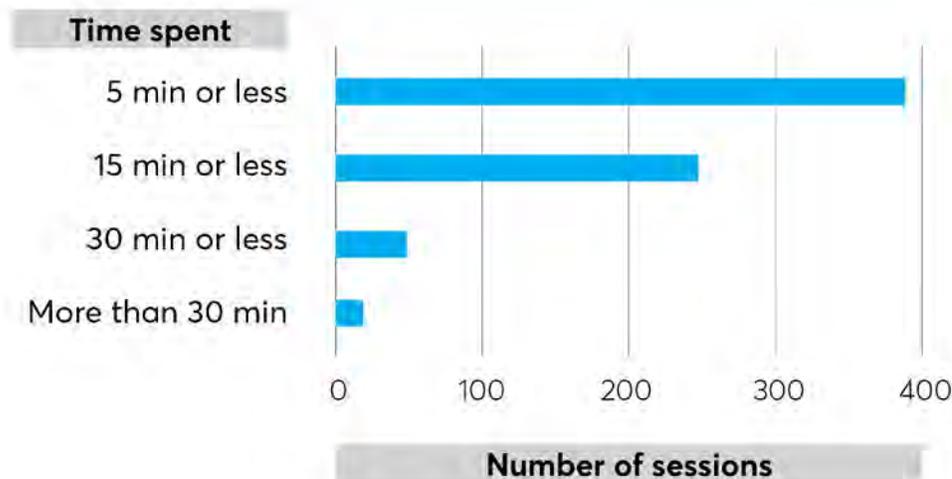
We also asked consumers about how long they spent to complete a request, and to not include the time spent filling out the survey. While the vast majority of consumers spent less than 15 minutes at a time on requests—and the most common amount of time was less than 5 minutes—some consumers reported that they nearly an hour or more than an hour opting out. A consumer working on the Jun Group reported that they were required to obtain their advertising ID to opt out: “Obtaining my Advertising Identifier was very time consuming and I am not sure how it is used.” The consumer testing Accuity reported: “They make it so hard to even find anything related to my information collected or subscribing or op-out that I had to read through so much boring yet infuriating do to what they collect and every one the will give it to for a price. We, as

⁵⁷ ACBJ (last visited Aug. 10, 2020), <https://acbj.com/privacy#X>.

Americans shouldn't have to do this to keep our information out of advertising collectors.”

Even spending five minutes on a single opt-out request could prevent consumers from exercising their CCPA rights. A consumer would have to make hundreds of such requests to be opted out of all data brokers potentially selling their data—not to mention all of the other companies with which the consumer has a relationship.

Sessions By Time Spent



At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.

Participants reported giving up in 7% of tests.⁵⁸ They reported being unable to proceed with their request in another 7% of tests.⁵⁹ These 14% of cases represent a DNS process clearly failing to support a consumer's CCPA rights.

⁵⁸ Example responses coded as “giving up” include: “Dead ended, as I am not going to send the info requested” and “Gave up because too frustrating. . . ”

⁵⁹ Example responses coded as “unable to proceed” include “the website is currently waiting for me to provide my IDFA number but I'm not sure how to adjust my settings to allow the new app permissions to retrieve;” “I could not Submit my form after several tries;” and “It looks like I did not email them after

The overwhelming reason for a consumer to refrain from part of a DNS request process, or give up all together, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: "I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty." Even consumers that ended up providing the drivers' license ended up confused by the company's follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: "After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that '[w]e will update the ranges in the future release.' I have no idea what that means." Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.

The data broker X-Mode used data submitted as part of a DNS request to deliver a marketing email, a practice that is prohibited by the CCPA.

X-Mode, a data broker that sells location data, used customer data provided to opt out in order to send a marketing email, in violation of the CCPA. Study participants voiced concerns about handing over additional personal information to data brokers in order to protect their privacy, and it was disappointing to discover that their concerns were warranted. Consumers are particularly sensitive about receiving additional marketing messages. One consumer, for example, shared with us that they began receiving more unsolicited robocalls after submitting the opt-out request. Reflecting these concerns, the CCPA specifically prohibits companies from using data collected to honor an opt-out request for any other purpose.⁶⁰

getting nowhere calling the number on their website that was supposed to handle requests and had no idea what I was talking about."

⁶⁰ Cal. Civ. Code § 1798.135(a)(6).

But X-Mode ignored that requirement. X-Mode is a data broker that pays apps—such as weather and navigation apps—to collect location data from devices that have installed the software.⁶¹ X-Mode makes money by selling insights drawn from that data to advertisers. For example, the Chief Marketing Officer of X-Mode explained, “If I walked by a McDonald’s but walk into a Starbucks, my device knows with the XDK that I passed a McDonald’s but I actually went into Starbucks.”⁶² X-Mode also sells personal information to third party applications and websites.⁶³ And it has also shared anonymized location data with officials in order to help track compliance with stay-at-home orders during the COVID-19 crisis.⁶⁴ Because it sells such sensitive information, X-Mode should be particularly careful to protect the anonymity of consumer data and respect consumers’ privacy preferences.

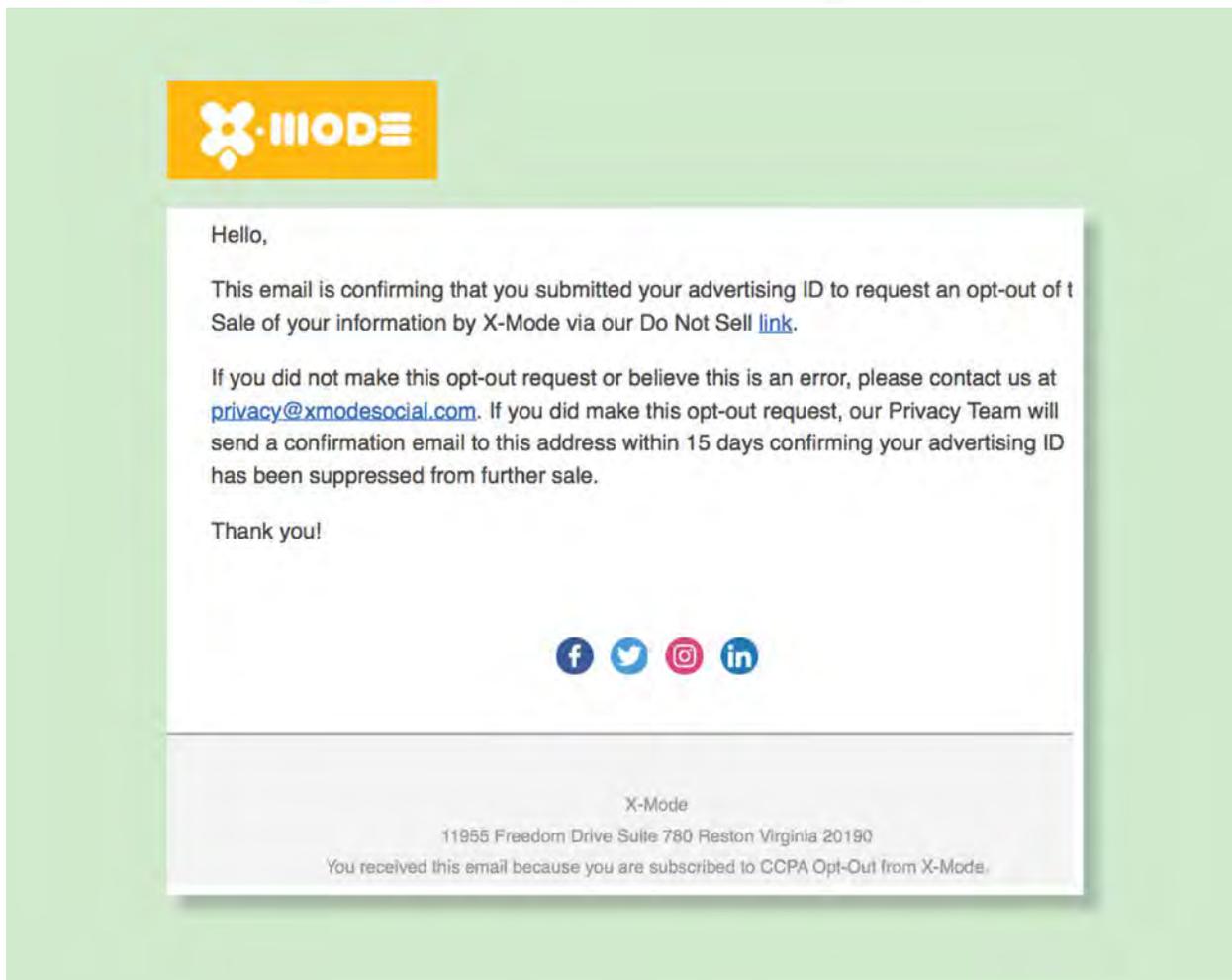
After submitting the opt-out request in April 2020, the author received the following email confirming that she had been placed on an “CCPA Opt-out” mailing list:

⁶¹ Sam Schechner et al., *Tech Firms Are Spying on You. In a Pandemic, Governments Say That’s OK*, WALL ST. J. (June 15, 2020), <https://www.wsj.com/articles/once-pariahs-location-tracking-firms-pitch-themselves-as-covid-sleuths-11592236894>.

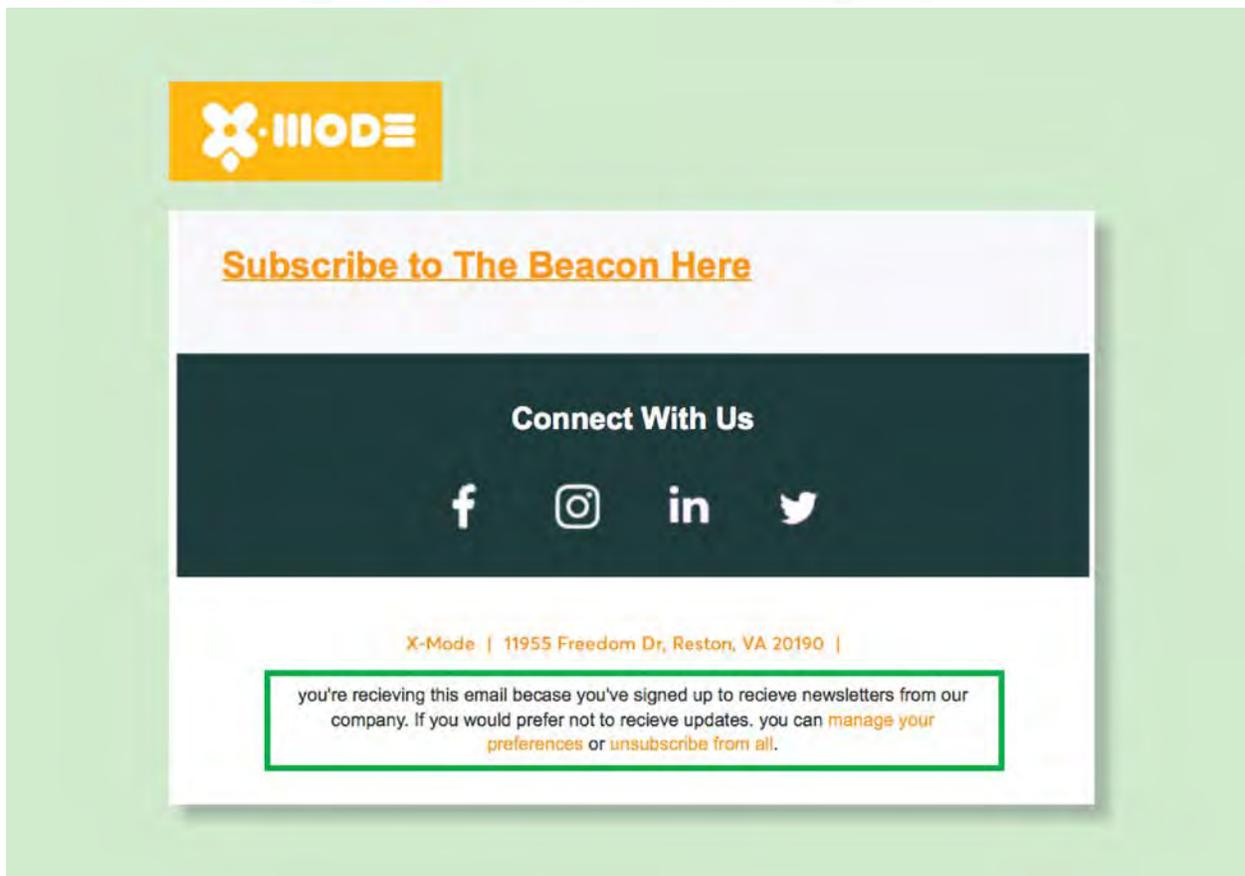
⁶² Jake Ellenburg, quoted in Karuga Koinange, *How Drunk Mode, An App for the Inebriated, Became Data Location Company X-Mode Social*, TECHNICALLY (Feb. 27, 2020), <https://technical.ly/dc/2020/02/27/how-drunk-mode-app-became-data-location-company-x-mode-social/>.

⁶³ ZenLabs LLC, Privacy Policy (last visited Aug. 28, 2020), <http://www.zenlabsfitness.com/privacy-policy/>.

⁶⁴ Schechner et al., *Tech Firms Are Spying on You*, *supra* note 61.



The following month, the author received an email inviting her to subscribe to X-Mode's newsletter in order to keep up with the business. The fine print explained that the email was sent "because you've signed up to receive newsletters from our company[,] with the option to unsubscribe.

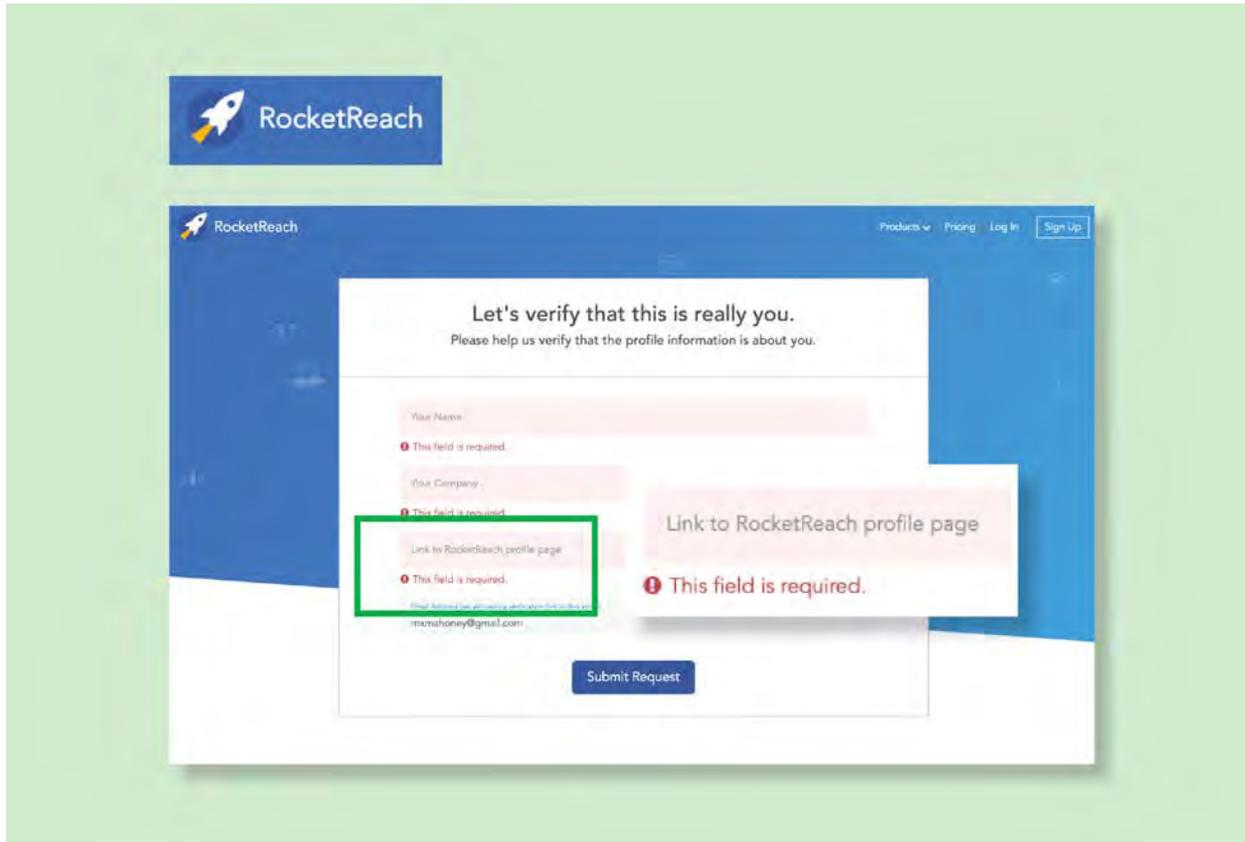


Since the only interaction that the author has had with X-Mode was to opt out—by definition, data brokers do not have relationships with consumers—the only way that she could have “signed up” was through opting out of the sale of her information. This behavior violates the CCPA’s prohibition on reuse of data provided for exercising data rights, and it could have a chilling effect on consumers exercising their rights with respect to other companies, as they are understandably worried about subjecting themselves to even more messages.

The data broker RocketReach requires the user to set up an account to opt out, which is prohibited by the CCPA.

RocketReach, a company that helps users find the contact information of potential business leads, requires users to list their RocketReach account in order to opt out of the sale of their information, even though the CCPA explicitly prohibits requiring

consumers to set up an account to opt out.⁶⁵ The homepage includes a link that reads “Do Not Sell My Info,” which then takes the consumer to a page that requires them to list their name, company, link to RocketReach profile, and email. If the user enters only name and email, the site does not let the user proceed further.



This frustrated testers, one of whom said, “I cannot determine whether they hold any of my information because they require a company and RocketReach account profile in order to honor the do not sell request.”

About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.

Neither the CCPA nor the implementing regulations require companies to notify consumers when their opt-out request has been honored, and this left consumers

⁶⁵ Cal. Civ. Code § 1798.135(a)(1).

confused about whether the company was still selling their information. Only in 18% of requests did participants report a clear confirmation from the broker that their data was or would soon not be sold. **In 46% of tests, participants were left waiting or unsure about the status of their DNS request.** In the 131 cases where the consumer was still waiting after one week, 82% were dissatisfied with the process (60% reported being very dissatisfied, and 22% reported being somewhat dissatisfied). The lack of clarity and closure was reflected in consumer comments such as “left me with no understanding of whether or not anything is going to happen” and “While it was an easy process—I will read their privacy policy to see if there is more [I] have to do to verify they are complying with my request. They left me unsure of the next step.”

In looking at how often consumers gave up or were unable to complete requests, we found a wide variety of responses from brokers, and variation in how consumers interpreted those responses. Once a DNS request was submitted, broker responses included:

- no response at all;
- acknowledging the request was received but providing no other information;
- acknowledging the request was received and vague language leaving consumers unsure of what was next;
- saying the request would be implemented in a certain timeframe (ranging from 2 weeks to 90 days);
- asking consumers to provide additional information;
- confirming a different type of request (such as Do Not Contact or Do Not Track);⁶⁶
- telling the consumer that the broker is not subject to the CCPA (even though the company was listed on the California data broker registry);
- telling the consumer that the broker has no data associated with them; and
- acknowledging the request was received and confirming that data will no longer be sold.

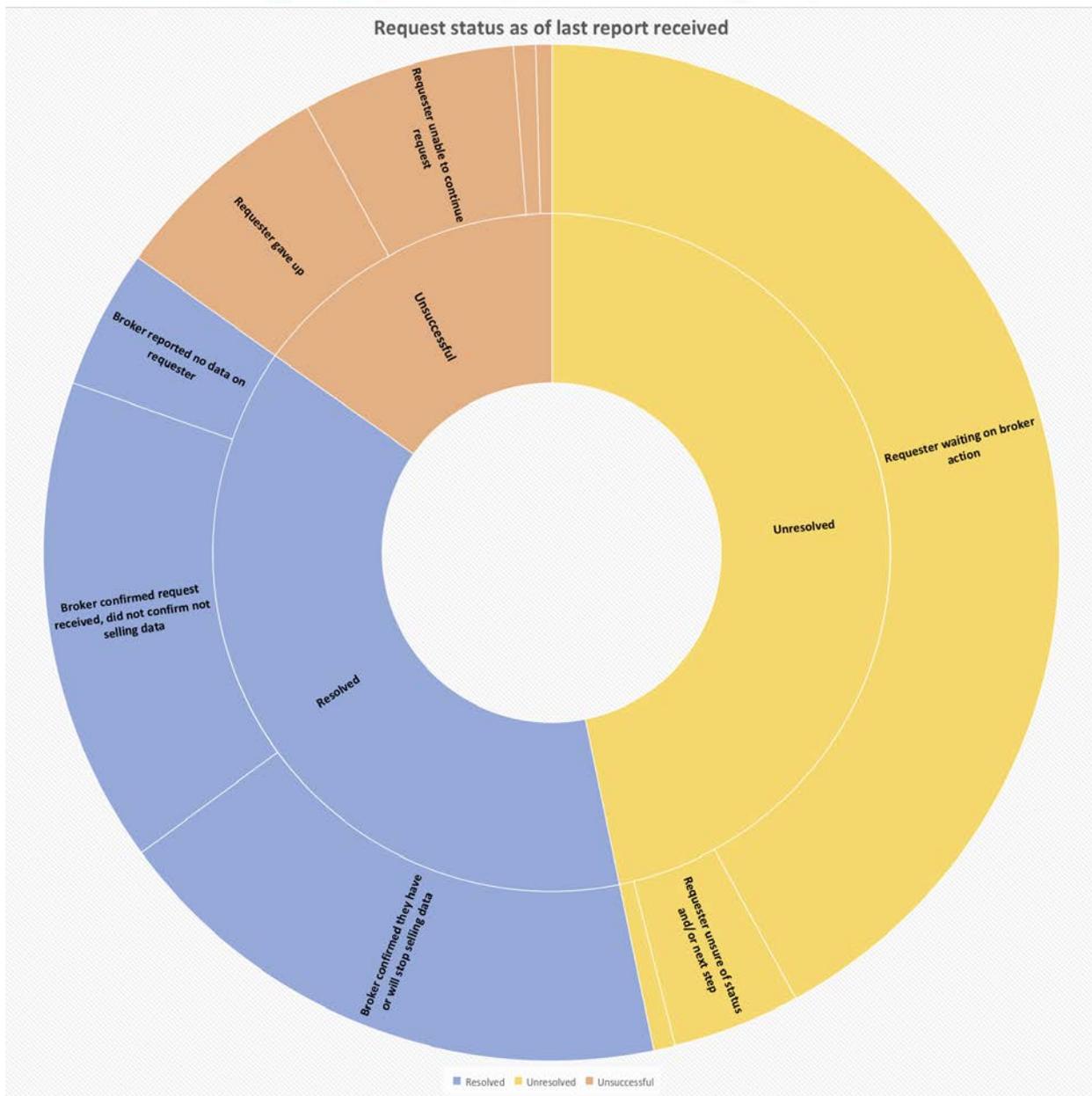
Consumers' understanding of these responses varied. For example, among participants reporting that the broker said that their request was received and that it would be

⁶⁶ Testers' references to “Do Not Contact” likely refer to consumers' right to be added to a company's internal “Do Not Call” list under the Telemarketing Sales Rule, 16 CFR § 310.4(b)(1)(iii)(A). Do Not Track refers to a request to stop tracking information about a consumer's activity across multiple sites. California law requires companies that collect personal information to disclose in the privacy policy whether they honor Do Not Track. See Cal. Bus. Prof. Code § 22575(5).

implemented in a certain time frame, some said the broker was honoring their DNS request but most said they were still waiting or unsure of the status of their request.

Below is a chart and visualization of the proportions of requests with different statuses as of the last report for each request:

Overall Status	Sub Status	Number Requests
Resolved	Broker confirmed they have or will soon stop selling data	107
	Broker confirmed request received, did not confirm not selling data	91
	Broker reported no data on requester	26
Unresolved	Requester waiting on broker action	247
	Requester unsure of status and/or next step	24
	Requester has outstanding follow up	4
Unsuccessful	Requester gave up	42
	Requester unable to continue request	40
	Broker reported not subject to CCPA	4
	Broker confirmed non-DNS request	3



We took a closer look at requests in which participants were “waiting” as of their last report, and found that many were still waiting for the data broker to respond to them after 21 days. Among the 247 requests in which the consumer was waiting for broker action, 81 were waiting after 21 days, 50 were waiting after at least a week but less than 21 days, and 116 of these were within 2 days of initiating a request. Those 116 represent cases where the broker may follow up later. However, the 81 cases in which consumers were still awaiting broker action after 21 days represent a problem with the

CCPA, in which consumers must choose between giving up and staying engaged for weeks at a time in hopes of receiving a clear confirmation from the broker that their DNS request has been completed. In 17 requests, the tester reported in an open-ended answer that they had had no response at all from the broker. Seven of these reports were after 21 days, and another 4 were after at least one week.

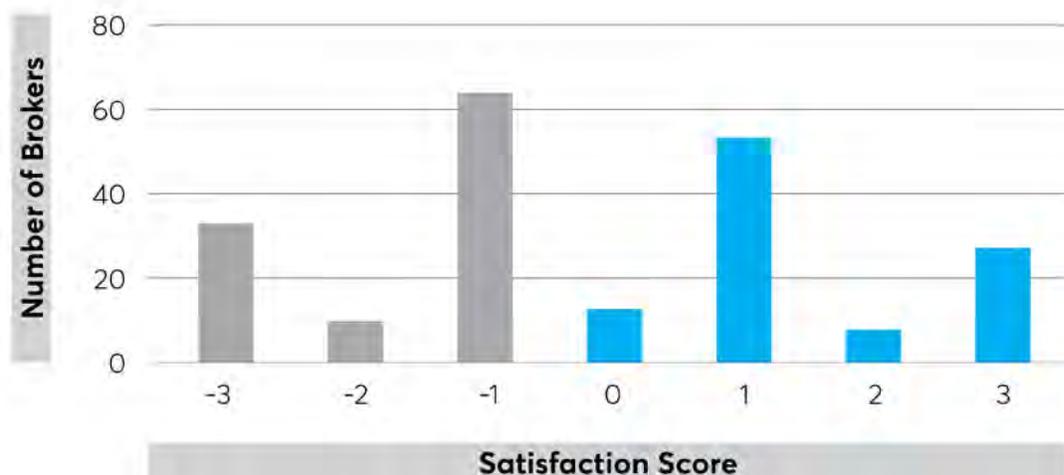
About 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with opt-out processes.

Overall, testers were more often dissatisfied than satisfied with the DNS processes. The survey asked how satisfied testers were with the process by providing four answers: very satisfied, somewhat satisfied, somewhat dissatisfied, very dissatisfied. The question was optional. Of the testers who answered this question, about 52% of the time, the tester was somewhat or very dissatisfied, and about 47% of the time, the tester was very or somewhat satisfied.⁶⁷

We also assigned each broker a satisfaction score. Some companies had consistent satisfaction, others had consistent dissatisfaction, and most had processes leaving consumers mixed in their satisfaction levels. In the satisfaction score, a broker received a positive point for a “very satisfied” or “somewhat satisfied” answer, and a negative point for a “somewhat dissatisfied” or “very dissatisfied” answer. The number of brokers with each score is plotted on the next page.

⁶⁷ Testers answered this question in 601 tests. Of these tests, in 317 (52%), the respondent was “somewhat dissatisfied” or “very dissatisfied” with the opt-out process, and in 284 (47%) tests, the respondent was “very satisfied” or “somewhat satisfied.” In 41 cases, the tester did not answer the question.

Tester Satisfaction



Some data brokers had quick and easy opt-out processes, showing that companies can make it easier for consumers to opt out. About 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

In several cases, consumers reported either a one-step process using an online interface that confirmed their data would no longer be sold, or a prompt and clear confirmation via email from the broker that their data would no longer be sold. For example, one tester of American City Business Journals described the process: “Just had to go to the privacy link at the bottom of the home page. Found the Calif. privacy link then had to scroll to button to turn off 'sell my info'.” Another shared an email from a DT Client Services, received the same day she submitted her request, that clearly confirmed that they would stop selling her data: “We confirm that we have processed your Request and will not sell your personal information to third parties.” These processes demonstrate an effective standard for implementing DNS requests. Overall, about 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

It is also possible for data brokers to post DNS links that are easy to find. For example, for 58% of the brokers, all three testers found the DNS link on the broker’s website, suggesting that these links were posted prominently. Links that were easy to find were

described as “prominent and easy to find,” “at bottom of page, but large,” “bottom of page, bold,” and “prominent at bottom of home page.” Thirty-nine data brokers out of 214 had all three testers report that the DNS link was “very easy” to find. For brokers where three out of three testers found the DNS link, the link was reported “very easy” or “somewhat easy” to find in 65% of cases, and “very difficult” or “somewhat difficult” to find in only 13% of cases.

Policy recommendations

The Attorney General should vigorously enforce the CCPA to address noncompliance.

The AG should use its enforcement authority to address instances of noncompliance, and to incentivize other companies to comply. While the AG is hamstrung by flaws in the enforcement provisions of the privacy requirements, notably the “right to cure” language that lets companies off the hook if they “cure” the problem within 30 days,⁶⁸ taking action will help push companies to get into compliance. Our study showed that a few improvements would go a long way. For example, it was significantly easier to opt out of a data broker site when the company had a link clearly labeled “Do Not Sell My Personal Information” that took consumers directly to the interactive form. Once that element was removed, consumers were often adrift, forced to email customer service staff who may not understand the request, or sent through a maze of sites with confusing disclosures. The AG should make an example of companies that fail to meet these requirements to help bring all of them into compliance.

To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales with a single step.

At the very least, consumers need access to universal opt-out tools, like browser privacy signals. Requiring consumers to opt out of every company one-by-one simply is not workable. The AG regulations require companies to honor platform-level privacy signals as universal opt outs, if the signal clearly constitutes a “Do Not Sell” command.⁶⁹ At the moment, however, there are no platform signals that we are aware of that clearly indicate a desire to out of the sale of data. Browsers are a logical place to start, though consumers need ways to opt out of advertising on devices other than browsers, such as

⁶⁸ Cal. Civ. Code § 1798.155(b).

⁶⁹ Cal. Code Regs. tit. 11 § 999 315(c) (2020).

TVs and phones. The AG should encourage developers to bring to market these solutions as quickly as possible, and should also set up a registry to help identify the signals that must be honored. This would help bring clarity for businesses and consumers.

The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.

Given that many consumers found it difficult to find the Do Not Sell link—it was often labeled with something different, and often buried at the bottom of the page with a bunch of other links—a graphic button would likely have value in ensuring that consumers would take advantage of that privacy protection. The CCPA directs the AG to design an opt-out button: “a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.”⁷⁰ The AG designed an initial draft, but declined to include a design in the final regulations. According to the AG, the proposed opt-out button was “deleted in response to the various comments received during the public comment period. The OAG has removed this subsection in order to further develop and evaluate a uniform opt-out logo or button for use by all businesses to promote consumer awareness of how to easily opt-out of the sale of personal information.”⁷¹ While the original design came under a fair amount of criticism, a uniform button, regardless of what it ends up looking like, will likely have value for consumers seeking to opt out, and the AG should promulgate one as soon as possible.

This will also help address instances in which companies route consumers through multiple, unnecessary steps in order to opt out. For example, Outbrain (*infra*, p. 18) led consumers through multiple steps to opt out, and on nearly every page the consumer had to hunt to figure out which option would lead them to the next step. And after all that, at least one consumer told us that they were not sure they had even opted out. Given that 7% of our testers gave up on the opt outs out of frustration or concern about sharing additional information, confusing interfaces significantly undermined consumers' ability to opt out.

⁷⁰ Cal. Civ. Code § 1798.185(a)(4)(C).

⁷¹ FSOR, *supra* note 27, at 15.

The AG should require companies to notify consumers when their opt-out request has been honored.

Many consumers had no idea whether or not their opt-out request had been honored. The uncertainty often left consumers dissatisfied with the opt out. Some companies did notify consumers that their requests had been honored, and this information was characteristic of simple, quick, and effective opt-out processes.

Required notification is also important for compliance purposes. For example, the AG regulations require companies to comply with opt outs within 15 business days. Without providing any notification of the opt out completion, there's no way to judge whether or not the company has honored the law and to hold them accountable if not.

The legislature or AG should clarify the definitions of “sale” and “service provider” to more clearly cover data broker information sharing.

In response to the CCPA, many companies have avoided reforming their data practices in response to “Do Not Sell” requests by arguing that data transfers either are not “sales,” or that transferees are “service providers” such that opt-out rights do not apply.⁷² Certainly, while some sharing with true data processors for limited purposes should not be subject to opt-out requests, many companies' interpretation of the CCPA seems to argue that third-party behavioral targeting practices are insulated from consumer choice.⁷³ As such, even if a consumer successfully navigates a DNS request from a data broker, in practice exercising opt-out rights may have little to no practical effect. Policymakers should close these potential loopholes to clarify that, *inter alia*, data broker information sharing for ad targeting is covered by CCPA obligations.

Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.

⁷² Mahoney, *Companies Aren't Taking the CCPA Seriously*, *supra* note 5.

⁷³ IAB CCPA Compliance Framework for Publishers & Technology Companies, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf; Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019), <https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175>.

While our study demonstrates that too many companies do not appear to be complying in good faith with the CCPA, any model that relies upon individuals to affirmatively act to safeguard their privacy will be deeply flawed. Given the challenges posed to businesses and consumers with respect to opting out, a better model is to ensure that privacy is protected without the consumer having to take any additional action. Several consumers who signed up for the study expressed shock that they were expected to opt out of the sale of their information. The thought of having to work their way through the entire data broker registry, which had hundreds of companies, was near unimaginable for these participants. Hard-to-find links, if they're even posted at all, confusing opt-out processes, requiring consumers to submit additional personal information, and above all the fact that there are hundreds of data brokers on the registry alone—all suggest that the responsibility needs to be on the company to protect privacy in the first place, rather than placing all the responsibility on the consumer.

This is a particularly important issue for elderly consumers or others who may have difficulty navigating online, several of whom dropped out of our study because it was so challenging to complete a single opt out. While there may be an easier path forward for some consumers who are able to take advantage of browser privacy signals to opt out universally—those are people who are already fairly tech savvy in the first place. Further, such a system only limits the sale of online data or data collected via a platform; it wouldn't stop the sale of data collected, say, in physical stores.

A better model would simply be to prohibit the sale of personal information as a matter of law, and to mandate that companies only collect, share, use, or retain data as is reasonably necessary to deliver the service a consumer has requested. Consumer Reports has supported legislation to amend the CCPA, AB 3119 (2020), that would require just that; Senator Sherrod Brown has introduced similar legislation, the Data Accountability and Transparency Act of 2020, at the federal level.⁷⁴ While the CCPA and the California data broker registry law are important milestones that improve transparency and individual agency, ultimately a more robust approach will be needed to truly protect Californians' privacy.

⁷⁴ The Data Accountability and Transparency Act of 2020, Discussion Draft, <https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf>.

Conclusion

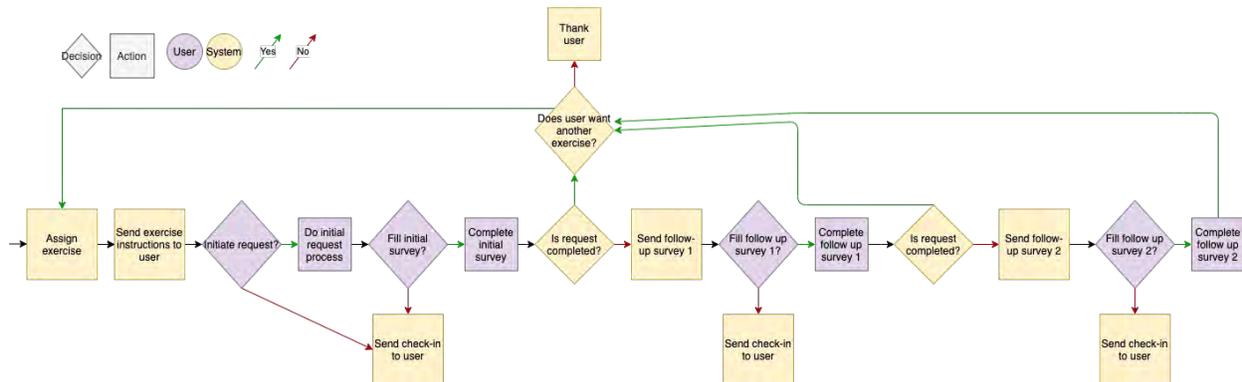
Overall, we found that consumers were too often dissatisfied with CCPA opt-out processes. This study uncovered some cases where the DNS process was short, clear, and satisfactory. It also found that some companies aren't complying with the CCPA, and that consumers were often left frustrated and without confidence that they had successfully exercised their DNS rights. It also reveals that, too often, consumers were unable to make a DNS request or gave up on the process altogether. Policymakers need to adopt crucial reforms in order to ensure that consumers can enjoy their right to privacy under the California Constitution.⁷⁵

⁷⁵ Cal. Cons. § 1.

Appendix

Section A

Below is a diagram of the participant experience of the exercise. Participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that broker. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker.



Section B

Below, we include links to screenshots of the homepages of data brokers that did not have the required "Do Not Sell My Personal Information" links on their homepages.

[adMarketplace, Inc.](#)
[Big Brook Media, LLC](#)
[Blue Hill Marketing Solutions, Inc.](#)
[Comscore, Inc.](#)
[Electronic Voice Services, Inc.](#)
[Enformion, Inc.](#)
[Exponential Interactive, Inc. doing business as VDX.tv](#)
[Gale](#)
[GrayHair Software, LLC](#)
[Infinite Media Concepts Inc.](#)
[JZ Marketing, Inc.](#)
[LeadsMarket.com LLC](#)
[Lender Feed LC](#)
[On Hold-America, Inc. DBA KYC Data](#)
[Outbrain Inc.](#)
[PacificEast Research Inc.](#)
[Paynet, Inc.](#)
[PossibleNow Data Services, Inc](#)
[RealSource Inc.](#)
[Social Catfish LLC](#)
[Spectrum Mailing Lists](#)
[SRAX, Inc.](#)
[USADATA, Inc.](#)
[zeotap GmbH](#)

Section C

An additional five companies had “Do Not Sell” links on their homepages, but all three testers were unable to find the DNS link, suggesting that it may not have been posted in a “clear and conspicuous manner” as required by the CCPA. Below, we include links to screenshots of the homepages of these companies.

[AcademixDirect, Inc.](#)

[Fifty Technology Ltd.](#)

[Freckle I.O.T. Ltd./PlacelQ](#)

[Marketing Information Specialists, Inc.](#)

[Media Source Solutions](#)

From: [Kammerer, Susan](#)
To: [Privacy Regulations](#)
Cc: [Merz, Jeremy](#)
Subject: APCIA Comments
Date: Wednesday, October 28, 2020 10:52:22 AM
Attachments: [image003.png](#)
[CA CCPA Regulations - Third Round - APCIA Comments - Final.pdf](#)

To Whom it May Concern:

Thank you for the opportunity to provide comments on the California CCPA regulations.
Please see APCIA's attached comment letter.

Thank you,

Susan Kammerer
Administrative Assistant
APCIA
1415 L Street, Suite 670
Sacramento, CA 95814





October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 S. Spring St., First Floor
Los Angeles, CA 90013

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

Dear Lisa Kim:

The American Property Casualty Insurance Association (APCIA)¹ appreciates the opportunity to provide comments on the Third Set of Proposed Modifications to the California Consumer Privacy Act Regulations (Proposed Revisions). We respectfully provide recommendations for your consideration below.

999.306(b)(3) – Notice of Right to Opt-Out of Sale of Personal Information.

The Proposed Modifications in subsection (3) may create compliance uncertainty and consumer confusion in a circumstance where the business separately collects information on-line and off-line. For example, a business may only sell personal information it collects about online website users or from internet-enabled technology devices. Nonetheless, if that business separately collected personal information offline that is not sold, it would be required to notify offline consumers of the sale of online information. This could be confusing for consumers. As such, APCIA recommends changing “collects personal information” to “sells personal information it has collected.” Thus, the requirement and illustrative examples would be appropriately limited to businesses that sell personal information they have collected, either online or offline.

W383-1

999.315(h) – Requests to Opt-Out

Subsection (h) provides a list of illustrative examples that clarify what is considered an easy opt-out procedure that does not subvert or impair consumer choice and utilizes minimal consumer steps. APCIA

W383-2

¹ APCIA is the preeminent national insurance industry trade association, representing property and casualty insurers doing business locally, nationally, and globally. Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of all sizes, structures, and regions of any national trade association.

believes the examples are prescriptive and unnecessary. For instance, subsection (1) places an arbitrary requirement that the steps a consumer is required to take for executing an opt-out cannot be greater than those required to opt-in. This does not account for different technological components involved in completing those choices. Further, subsection (h)(3) is contrary to other privacy requirements that a business explain the impacts of a consumer's privacy choice. As an alternative, the illustrative examples should become factors in determining whether an opt-out method is permissible. This is a more flexible approach that will allow companies to meet the requirements without being faced with impossible choices about privacy disclosures or effective technology solutions.

W383-2
(cont)

W383-3

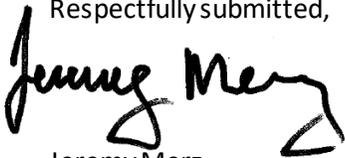
999.326(a) – Authorized Agent

The Proposed Revisions are positive in that they promote more choice and flexibility in agent authorization practices, while retaining the ability to require the consumer to verify their identity as necessary.

W383-4

Thank you for the opportunity to comment. Please let us know if you have any questions or would like additional information.

Respectfully submitted,



Jeremy Merz
Vice President, State Government Relations



From: [Dale Smith](#)
To: [Privacy Regulations](#)
Subject: CCPA Written Comment on Proposed Regulations Due October 28 (Transmitting)
Date: Wednesday, October 28, 2020 11:51:56 AM
Attachments: [footerNew2.bmp](#)
[20201028 CCPA Comments.pdf](#)

Dear Privacy Regulations Coordinator:

Attached to this email is our .pdf document containing PrivacyCheq's submission of comment for NOTICE OF THIRD SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS, released October 12, 2020 (comment period closing on October 28).

Thank you for this opportunity to comment.

Dale Smith

DALE R. SMITH, CIPT

Futurist | 



View my blog at: privacyelephant.com



October, 28, 2020

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Via Email to: PrivacyRegulations@doj.ca.gov

Attn: Honorable Xavier Becerra, Attorney General

Re: Comments on NOTICE OF THIRD SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS, Released October 12, 2020

Dear Mr. Becerra:

The newly added section §999.306(b)(3)(a) sets forth an illustrative example of how a consumer can be made aware of the right to opt-out in a brick-and-mortar, offline situation. It suggests using a printed paper form and/or by posting appropriate signage.

We are commenting to point out that both of these methods can be operationally enhanced if combined with the use of a QR code¹ and just-in-time notice in conjunction with the paper form or signage. Addition of the QR code technology can bring interactivity between business and consumer even in an offline setting.

W384-1

¹ https://en.wikipedia.org/wiki/QR_code

A fictitious example can demonstrate how this works. Figure 1 below visualizes one of the many ways a QR code might be deployed for use in an offline retail setting. Here, the content of the signage is static and venue-specific, but the addition of the QR code gives life to a “just-in-time” interactive notice readily available to the consumer.



Figure 1

Seconds after the consumer “shoots” the QR code on the signage using his smartphone app², a §999.306-compliant notice will appear on the consumer’s phone, ready to interactively inform the consumer of appropriate CCPA rights and choices.

²

<https://www.google.com/search?q=smartphone+qr+scanner+app&oq=qr+smaratphone+app&aqs=chrome.1.69i57j0i22i30i457j0i22i30l3j0i8i13i30l2.16643j0j7&sourceid=chrome&ie=UTF-8>

Figure 2 illustrates how that smartphone screen might look.

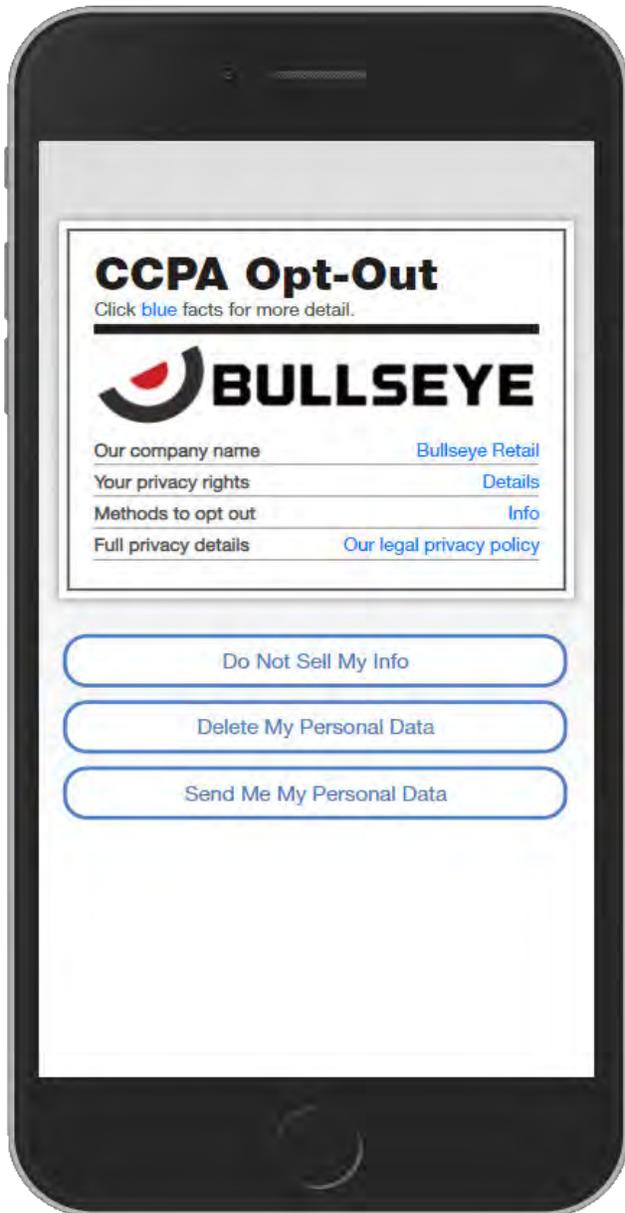


Figure 2

As before, the content of this fictitious screen visualizes several of the many ways an interactive notice can put consumers in the driver's seat regarding their privacy choices. In this example, in addition to presenting drill-down §999.306-specific information, the Do Not Sell, Access, and Deletion rights are set forth as options on the notice's front page.

W384-1
cont



This scenario demonstrates how the addition of public domain QR technology can transform a retail pamphlet or mall sign into an opportunity for a consumer to interact easily and directly with a business in real time to understand and take advantage of privacy rights provided by CCPA.

Regarding our specific comment, we suggest that in order to enrich the illustrative examples referenced in §999.306(b)(3), verbiage should be added to §999.306(b)(3)(a) mentioning the utility of the QR code concept as an efficient and practical means of informing consumers in offline environments.

W384-1
cont

Use of a QR “trigger” to deliver on-demand, “just-in-time” notices also meets the purpose under §999.305(a) Notice of Collection and §999.307(a) Notice of Financial Incentive.

Additional information on practical CCPA just-in-time notice implementation can be found in PrivacyCheq’s previous comment submissions to the CCPA Proposed Regulation which closed on [December 6, 2019](#), [February 24, 2020](#), and [March 27, 2020](#).

Finally, we respectfully reiterate our previous suggestion that the ubiquitous Nutrition Label framework be named within the regulations as an example of a readily adaptable standard and functional implementation of what is called for in §1798.185(a)(4)(C)³.

W384-2

We thank you for these opportunities to comment.

A handwritten signature in black ink, appearing to read 'D.R. Smith', with a long, sweeping flourish extending to the right.

Dale R. Smith, CIPT
Futurist

³ §1798.185(a)(4)(C) The development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.

From: [Emery, Emily](#)
To: [Privacy Regulations](#)
Cc: [Emery, Emily](#)
Subject: MPA Comments on the Third Set of Proposed Modifications to Text of CCPA Regulations
Date: Wednesday, October 28, 2020 1:19:02 PM
Attachments: [MPA Comments on Modifications to CCPA Rulemaking 10.28.2020.pdf](#)

Attached, please find comments on the third set of proposed modifications to the text of regulations implementing CCPA submitted on behalf of MPA - The Association of Magazine Media.

We appreciate the opportunity to provide the attached comments for your consideration.

Emily Emery
Director of Digital Policy
MPA - The Association of Magazine Media
Cell: [REDACTED]
Office: [REDACTED]
[REDACTED]

October 28, 2020

The Honorable Xavier Becerra
California Department of Justice
ATTN: Lisa B. Kim, Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

Submitted via email to PrivacyRegulations@doj.ca.gov

RE: Comments from MPA – the Association of Magazine Media on the Third Set of Proposed Modifications to Text of Regulations Implementing the California Consumer Privacy Act (CCPA) OAL File No. 2019-1001-05

Dear Attorney General Becerra:

MPA – the Association of Magazine Media represents over 500 magazine media brands that deliver compelling and engaging content across online, mobile, video and print media. MPA represents the interests of all types of magazine media companies, from the largest global companies to the smallest independent journal, and their news, business and finance, lifestyle, and enthusiast brands that appeal to a broad set of interests. Members of our industry connect with more than 90 percent of all U.S. adults through the digital and print magazine titles readers value most.

Having testified and provided previous rounds of comments on modified language proposed by the Office of the Attorney General (“OAG”), we appreciate the opportunity to offer additional comments on the third set of proposed modifications to the regulations implementing the California Consumer Privacy Act (“CCPA”).

Almost a full year into implementation of the CCPA, it is extremely important that the third set of proposed modifications not undermine the extensive efforts undertaken and procedures implemented by magazine media companies and others based on previous versions of the rulemaking. Further, consumers have now developed expectations regarding CCPA processes that should not be upended. In the sections below, MPA makes recommendations with respect to the OAG’s proposed modifications to requirements for offline notices, number of allowable steps for opt-out, and requests made through authorized agents. Please note that MPA’s suggested additions are indicated in ***bold italicized underline***.

I. The OAG should clarify in its modifications to Section 999.306(b)(3) that in instances where personal information is collected through a printed form that is to be mailed back to the company, the offline notice may include a web address that the customer can access to opt-out of the sale of their personal information

W385-1

In addition to collecting personal information online and at brick-and-mortar locations, the magazine media industry, as with other industries, may collect personal information that consumers complete through a printed form and then submit by mail.

To facilitate that common, expected consumer practice and enhance compliance with the aims of the CCPA, the OAG should confirm that in order to provide notice at the point of collection of personal information, it is sufficient for a business to direct a customer to a web address where the consumer may choose to instruct the business that sells personal information to stop selling their personal information.

MPA recommends that the OAG modify the proposed regulatory text in section 999.306(b)(3) to include an additional illustrative example:

(c) A business that collects personal information from consumers through printed forms by mail may provide notice by including on the paper forms that collect the personal information a web address directing consumers to where the consumer may choose to opt-out of the sale of their personal information.

W385-1
cont

This additional clarification – that the provision of a web address on printed material is an offline notice – would aid in compliance where consumer information is collected from a printed paper form that is then mailed by the consumer. This illustrative example for printed materials sent through the mail is consistent with existing regulation 999.305(b)(3) that offline notices may direct consumers to where the “Do Not Sell My Personal Information” webpage can be found online, and is analogous to the proposed illustrative example for brick-and-mortar stores (which may post signage).

This method of notice also enhances data privacy and security by minimizing the amount of data a business must collect in printed form in order to validate and execute a consumer’s request, allowing businesses to standardize operations, including the ability to have a single, centralized location where opt-out information is maintained.

II. The OAG should further clarify in 999.315 on requests to opt-out that two expected, common practices that enhance the consumer experience while promoting the minimal number of steps to opt-out are permitted.

MPA agrees that the steps for submitting a request to opt-out should be minimal and should not subvert consumer intent. However, MPA is concerned that requiring parity in the number of steps to opt-out and to opt-in could incentivize businesses to add additional steps to both the opt-in and opt-out process that do not enhance the consumer experience or privacy protections but merely ensure technical compliance with the CCPA, or present obstacles for businesses to employ standard identity verification processes that enhance consumer data security.

W385-2

MPA recommends that the OAG make the following additional modification to the proposed modifications to text in Section 999.315(h)(1):

- (1) **The business’s process for submitting a request to opt-out shall not require more steps than that business’ process for a consumer to opt-in to the sale of personal information after having previously opted out. A business’ process to validate a user’s identity shall not count in the number of steps to opt-in or opt-out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the “Do Not Sell My Personal Information” link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request, not including identity verification.**

W385-2
cont

Magazine media consumers often benefit from renewal offers that reduce the price of a subscription. Posting notice of an offer of a discounted subscription without creating an additional required step or friction for the consumer provides value to the consumer without impairing a consumer’s ability to execute their request to opt-out. The CCPA regulations should explicitly permit businesses to present a notice of benefits for the consumer should they elect to remain opted-in.

Consumers may also benefit from electing to opt-out of certain services or offerings while not opting-out entirely. Businesses should be permitted to enhance the consumer experience and better serve consumer intent by providing an easy opt-out process that allows the consumer to indicate his or her desired preferences. Businesses should be allowed to display an interface that enables the consumer to indicate a full or partial opt-out or select/de-select from a listing where multiple offerings exist as long as one of the de-selection options is inclusive of all of the business’ use of consumer data.

W385-3

MPA urges the OAG to add the following clarification to Section 999.315(h)(3):

- (3) **Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request. A business may display information that provides context to enable a consumer to reconsider their interest in opt-out or to elect a partial opt-out provided that display does not require additional steps or subvert or impair a consumer’s choice to opt-out. A display that provides an offer of additional goods or services shall not count in the number of steps to opt-out if the consumer is not required to take an action if they do not wish to take advantage of the offer.**

III. The OAG should strike its proposed modified language in Section 999.326(a) on authorized agents and continue to permit a business to exercise direct consumer engagement to effectively make good-faith efforts to respond to suspected threats to consumers’ data security.

The current CCPA text allows businesses to authenticate right to know and data deletion requests filed by either consumers directly or authorized agents, and to do so by presenting the same interface online for either method. For example, businesses currently commonly utilize a consumer’s email address to map to an account and process a request.

W385-4

Since the effective date of the CCPA, many businesses have identified practices by authorized agents that undermine consumers' data privacy and security. Therefore, MPA is concerned that the proposed language in Section 999.326(a) could impede the necessary steps that businesses would take to effectively respond to instances of suspected consumer fraud by purported authorized agents.

Reducing the avenues available for a business to obtain verification, particularly in instances of suspected fraud, both undermines consumer data security and is counter to the CCPA's authentication requirements found outside the section on authorized agents.

To maximize the protection of consumer data, a business must continue to have the ability to both directly verify identity with the person to whom the request is related, and to confirm that the consumer provided the authorization to the agent submitting the request.

MPA urges the OAG to restore the enacted text that allows businesses to exercise both verification methods:

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer:

(1) Provide the authorized agent signed permission to do so.

(2) Verify their own identity directly with the business.

(3) Directly confirm with the business that they provided the authorized agent permission to submit the request.

MPA again notes the important role that direct first-party engagement with consumers can have in enhancing data security, protecting privacy, and preventing fraudulent activity.

MPA believes that adopting the additional clarifications proposed above will enhance the ability of businesses, including the magazine media industry, to operationalize consistent privacy-protective practices that comply with the law, enhance reader trust, and preserve the viability of the magazine media brands that consumers enjoy.

MPA and our members appreciate the opportunity to provide our views for your consideration.

Respectfully submitted,

Brigitte Schmidt Gwyn
President and Chief Executive Officer

Rita Cohen
Senior Vice President, Legislative and Regulatory Policy

Emily Emery
Director, Digital Policy

From: [Leder, Leslie](#) on behalf of [Mohammed, Shoeb](#)
To: [Privacy Regulations](#)
Subject: Comments to Third Modified CCPA Regulations
Date: Wednesday, October 28, 2020 1:22:01 PM
Attachments: [FINAL CalChamber Comments to Third Modified CCPA Regulations.pdf](#)
Importance: High

Ms. Kim,

Attached please find CalChamber's comments to Text of Third Modified CCPA Regulations.

Thank you,

Shoeb Mohammed
Policy Advocate



California Chamber of Commerce
1215 K Street, 14th Floor
Sacramento, CA 95814

T [REDACTED]
F 916 325 1272

Visit calchamber.com for the latest California business legislative news plus products and services to help you do business.

This email and any attachments may contain material that is confidential, privileged and for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient or have reason to believe you are not the intended recipient, please reply to advise the sender of the error and delete the message, attachments and all copies.

October 28, 2020

SENT VIA EMAIL

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Written Comments to Third Set of Proposed Modifications to Text of CCPA Regulations
OAL File No. 2019-1001-05

SUMMARY

The California Chamber of Commerce (CalChamber) respectfully submits the following comments to the Attorney General's (AG) Third Set of Proposed Modifications to Text of California Consumer Privacy Act (CCPA) Regulations. As outlined in Section I, we believe this set of proposed modifications to the CCPA violates the APA and should be withdrawn. Sections II-IV outline concerns and substantive edits to the proposed modifications. Recommended revisions are formatted with additions in underline and deletions in ~~strikeout~~. Additionally, requests for clarification are outlined separately in Section V below.

COMMENTS

I. The Third Proposed Modifications Violate the Administrative Procedures Act

We believe the proposed amendments are unlawful and invalid because they violate the procedural requirements of California Government Code (GC) section 11340 et seq, the California Administrative Procedure Act (APA). GC 11346.4(b) provides that a Notice of Proposed Action is valid for one year. The 3rd proposed amendment was published on October 12, 2020, which is more than one year after the original the Notice of Proposed Action, which was dated October 11, 2019. Since 2020 is a leap year, the proposed 3rd amendments were published 367 days after the original Notice of Proposed Action.

The regulations implementing the California Consumer Privacy Act in this rulemaking were first submitted by the Department of Justice (DOJ) to the Office of Administrative Law (OAL) for review on June 3, 2020 (OAL Matter No. 2020-0603-03S). The outcome for this Matter was "Partial Approval, Partial Withdrawal". According to the Notice of Third Set of Proposed Modifications to Text of Regulations "[t]he Department withdrew the following sections from the review of the Office Administrative Law (OAL) pursuant to Government Code section 11349.3, subd. (c): 999.305(a)(5), 999.306(b)(2), 999.315(c), and 999.326(c)." The modified text published on October 12, 2020, proposes to add new regulatory language in sections 999.306(b)(3), 999.315(h), and 999.332(a), and to add and delete language in section 999.326(a). None of the

W386-1

provisions added or modified in the 3rd amendments modify the subdivisions which were originally withdrawn.

However, even if the 3rd amendments did modify subdivisions originally withdrawn, we believe it would still violate APA requirements. Regulations which are withdrawn during OAL review may be modified and resubmitted, but this must be done within the original one-year Notice period. The APA provides that regulations submitted to OAL may either be disapproved by OAL or withdrawn from OAL at the rulemaking agency’s request (GC 11349.3). The process for disapproval is defined by GC 11349.3(b). Withdrawal of a regulation by the rulemaking agency is regulated by GC 11349.3(c). Subdivision (c) provides, in part, that “Any regulation returned pursuant to this subdivision [i.e. a withdrawn regulation] shall be resubmitted to the office for review within the one-year period specified in subdivision (b) of Section 11346.4 or shall comply with Article 5 (commencing with Section 11346) prior to resubmission.”

The APA provides that a regulation disapproved by OAL may be resubmitted to OAL within 120 days of the disapproval. A regulation withdrawn by the submitting agency, in contrast, must be resubmitted to OAL, if at all, while the original one-year Notice remains valid. The 120-day extension that the APA provides for disapproved regulations does not apply to withdrawn regulations.

W386-1
cont

Since the 3rd amendments to the CCPA regulations were published after expiration of the original Notice of Proposed Action, they cannot possibly be “resubmitted to the office [OAL] for review within the one-year period specified in subdivision (b) of Section 11346.4.” Under GC 11349.3(c), the only way that these proposed regulations may be lawfully implemented is by “comply[ing] with Article 5 (commencing with Section 11346) prior to resubmission.” Article 5 requires, in essence, that a new Notice of Proposed Action be issued, a new 45-day public comment period occur, etc. In summary, to modify a withdrawn regulation, an agency must either resubmit the withdrawn regulation to OAL during the one-year life of the original Notice, or it must start the rulemaking process over from the beginning.

Accordingly, we respectfully request the Department to withdraw this Third Set of Proposed Modifications to Text of California Consumer Privacy Act (CCPA) Regulations and restart a new notice period under the APA.

II. SECTION 999.306 – Notice of Right to Opt-Out of Sale of Personal Information.

A. Issue: The requirement to provide notice by an offline method should only apply if information collected offline is sold.

1. Proposed Regulation: 999.306(b)(3)

§999.306(b) requires businesses to provide consumers with an offline method of opting out of the sale of personal information even if the businesses are not selling information that is collected offline. Businesses that do not engage in the practice of selling information shared offline should not be required to post signage implying that the information shared offline is subject to sale. Accordingly, this

W386-2

section should be narrowed in scope to apply only when businesses are collecting and selling information that is collected offline.

2. Recommended Change: Revise §999.306(b)(3) as follows:

(3) A business that collects personal information in the course of interacting with consumers offline and sells such information shall also provide notice by an offline method that facilitates consumers' awareness of their right to opt-out. Illustrative examples follow:

- a. A business that collects personal information from consumers in a brick-and mortar store and sells such information may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.
- b. A business that collects personal information over the phone and sells such information may provide the notice orally during the call where the information is collected.

W386-2
cont

B. Issue: The illustrative requirement to post signage in areas where personal information is collected may prohibit signage in more effective and noticeable locations.

1. Proposed Regulation: 999.306(b)(3)(a)

§999.306(b)(3)(a) requires businesses to post signage in the areas where personal information is collected. However, this could be read to prohibit businesses from prominently posting signage in high visibility areas such as store entrances and doorways if personal information is not necessarily collected at these points.

Further, the option to post signage “in the area where the personal information is collected” could be read to require signs at each point of sale or cash register in the state. In many stores, however, points of sale and cash registers are high interaction areas where consumers are not likely to see the notices. For this reason, it would be reasonable to allow businesses more options to post prominent signage.

2. Recommended Change: Revise §999.306(b)(3)(c) to illustrate that signage at the front door or similar prominent area is sufficient to satisfy the rule.

W386-3

III. SECTION 999.315 – Requests to Opt-Out.

A. Issue: The regulation prohibits businesses from providing essential disclosures of information that could be relevant and informative to users.

W386-4

1. Proposed Regulation: 999.315(h)

§999.315(h) prohibits businesses from requiring consumers to “click through” or “listen to reasons” why they should not submit a request to opt-out but fails to allow some reasonable degree of notice for the consumer. As drafted, the regulation prohibits additional disclosures of information that could be important, relevant and informative to users.

W386-4
cont

2. Recommended Change: Revise §999.315(h) to allow businesses to provide a reasonable degree of notice to the consumer.

IV. SECTION 999.326 – Authorized Agent.

A. Issue: Modifications will prohibit businesses from requiring two forms of identity verification when requests to know or delete information come from third parties.

1. Proposed Regulation: 999.326(a)

§999.326(a) requires businesses to choose between one of two forms of identity verification when a consumer uses an authorized agent to submit a request. Businesses should be allowed to use both forms of identity verification when authorizing consumer requests that come from third parties. As drafted, the regulation requires businesses to choose just one.

W386-5

2. Recommended Change: Restore §999.326(a) to previous draft.

V. Requests for Clarification

A. §999.315(h)(5): Request clarification about how this section aligns with the existing requirements in CCPA §1798.120(b) and §1798.115(d).

W386-6

B. §999.326(a): Request clarity about what “proof” is sufficient to evidence “signed permission to submit the request”

W386-7

Respectfully,



Shoeb Mohammed
California Chamber of Commerce

From: [Melanie Tiano](#)
To: [Privacy Regulations](#)
Subject: CTIA Comments on CCPA Modified Regulations
Date: Wednesday, October 28, 2020 1:46:07 PM
Attachments: [image003.png](#)
[10.28.20 CTIA Comments on CCPA Modified Regulations.pdf](#)

Hello,

Attached are CTIA's comments in response to the proposed modifications.

Please let me know if you have any questions.

Thank you,

Melanie Tiano



Melanie K. Tiano
Director, Cybersecurity and Privacy
1400 16th Street, NW
Washington, DC 20036
[REDACTED] (office)
[REDACTED] (mobile)

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of)
)
California Consumer Privacy Act) Public Forums on the California
Rulemaking Process) Consumer Privacy Act
)
)

COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036
(202) 736-3200
www.ctia.org

October 28, 2020

TABLE OF CONTENTS

INTRODUCTION	1
I. § 999.306 – Notice of Right to Opt-Out of Sale of Personal Information.....	2
a. The Department should clarify that the requirement for businesses to provide offline opt-out notices applies only where the information collected offline will be “sold” within the meaning of the CCPA.....	2
II. § 999.326 – Authorized Agent.....	4
a. The regulations should allow businesses to require that authorized agents verify their own identities.	4
b. The Department should clarify that the modified regulations permit businesses to require consumers to both verify their own identity and directly confirm that they have provided the authorized agent with permission.....	5

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL’S OFFICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act Rulemaking Process)	Public Forums on the California Consumer Privacy Act
)	

INTRODUCTION

CTIA appreciates the opportunity to provide these comments on the California Department of Justice’s (“Department”) Third Set of Modified Proposed Regulations (“modified regulations”) to implement the California Consumer Protection Act of 2018 (“CCPA” or “Act”).¹ CTIA recognizes the immense undertaking involved in drafting these regulations and commends the Department’s ongoing efforts to revise and clarify the final regulations.

Nevertheless, CTIA remains concerned about some of the provisions included in the modified regulations, particularly where certain aspects of the modified regulations remain unclear.

CTIA’s concerns pertain to the following sections:

- § 999.306 – Notice of Right to Opt-Out of Sale of Personal Information; and
- § 999.326 – Authorized Agents

Where appropriate, CTIA provides alternative regulatory language to address the issues identified herein.

¹ See generally Cal. Civ. Code § 1798.100 *et seq.*

I. § 999.306 – Notice of Right to Opt-Out of Sale of Personal Information

- a. The Department should clarify that the requirement for businesses to provide offline opt-out notices applies only where the information collected offline will be “sold” within the meaning of the CCPA.²**

Under the modified regulations at subdivision § 999.306(b)(3), any “business that collects personal information in the course of interacting with consumers offline” would be required to provide an offline opt-out notice to consumers. As written, this could be interpreted as requiring a business to provide an offline opt-out notice even where the business never “sells” the personal information it collects offline. Under this interpretation, this provision would have the unintended effect of misleading consumers into believing that their offline-collected personal information is “sold” when it is not, and further that consumers might stop these nonexistent data sales by exercising their CCPA opt-out rights.

For example, consider a major online and brick-and-mortar retail store that sells only the personal information it collects in connection with its online e-Commerce platform. As drafted, the modified regulations could be interpreted as requiring this business to provide an offline opt-out notice to consumers engaging in transactions at the store’s brick-and-mortar locations, provided that the business collects any personal information offline (e.g., loyalty account or payment card information) -- even when that information is not sold. Under this scenario, many offline consumers would reasonably, but mistakenly, believe that their offline-collected loyalty or payment card information will be sold unless they exercise their CCPA opt-out rights.

This interpretation is problematic for several reasons. If a retailer does not sell personal information it obtains offline, there is no need to provide an opt-out notice to the consumer. It is

W387-1

² Cal. Civ. Code 1798.140(t)(1) (stating that “‘sell,’ ‘selling,’ ‘sale,’ or ‘sold,’ means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration”).

confusing and misleading to notify the consumer of her right to grant or withhold consent to a transaction -- the sale of information -- that will never take place regardless of her election. CTIA understands that one of the Department's goals in issuing the regulations was to "promote greater transparency to the public regarding how businesses collect, use, and share personal information" and to "make it easier for consumers to exercise their rights."³ However, as described above, the suggested interpretation serves to obstruct both of these aims. Rather than promoting greater transparency, compliance with this provision would mislead consumers and add unnecessary confusion to the CCPA framework (i.e., consumers would frequently be confronted with offline opt-out notices which counterintuitively pertain only to personal information collected online). Moreover, rather than making it easier for consumers to meaningfully exercise their CCPA rights, it would make it harder for consumers to determine when to exercise those rights and to what information such an opt-out would apply.

W387-1
cont

CTIA therefore requests that the following clarifying language be inserted into subdivision 999.306(b)(3):

§ 999.306(b)(3). *A business that collects personal information in the course of interacting with consumers offline and sells such information shall also provide notice by an offline method that facilitates consumers' awareness of their right to opt-out. Illustrative examples follow:*

a. A business that collects personal information from consumers in a brick-and-mortar store and sells such information may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.

³ Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, State of California Department of Justice, Office of the Attorney General (Oct 11, 2019) <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf>.

b. A business that collects personal information over the phone and sells such information may provide the notice orally during the call where the information is collected.

W387-1
cont

II. § 999.326 – Authorized Agent

a. **The regulations should allow businesses to require that authorized agents verify their own identities.**

The current and modified regulations recognize the importance of verifying the identity of consumers making CCPA requests, however, they fail to recognize that verifying the identity of a purported authorized agent is equally important.⁴ While CTIA appreciates the Department’s recognition in subdivision § 999.326, that to better protect against fraudulent requests related to consumers’ personal information, businesses must be empowered to require agents to directly “provide proof that the consumer gave the agent signed permission to submit the request,” neither the regulations nor the proposed modifications expressly permit businesses to require that an authorized agent verify their own identity, which is an obvious hole in businesses’ ability to guard against fraudulent requests.⁵

W387-2

Given the relatively short time that the CCPA framework has been in place, it is unclear precisely how malicious actors will try to leverage requests to exploit consumers, but one likely possibility would be through fraudulent authorized agent requests. Accordingly, the CCPA regulations should grant businesses the flexibility to implement anti-fraud measures amid a rapidly changing cybersecurity landscape. One pillar of fraud protection would involve the vetting of authorized agents to confirm that, when a consumer legitimately exercises a CCPA request via an

⁴ CTIA also reiterates the concerns expressed in its March 27, 2020 comment that the powers of attorney exception in § 999.326(b) poses an unacceptable degree of risk to consumers. § 999.326(b) prevents businesses from deploying antifraud measures when presented with a document which many businesses will be unable to effectively verify.

⁵ For example, consider a consumer who has provided her authorized agent, “Agent A”, with authority to make a request on her behalf. Under the modified regulations, a business would be able to verify that, the consumer did in fact provide Agent A with such authorization, but would not be able to verify that the individual purporting to be Agent A, is actually Agent A.

authorized agent, the “agent” itself is, in fact, the authorized party to whom the consumer granted permission to make the request.

Failure to permit businesses to require agents to verify their own identity could result in fraud whereby fraudsters pose as authorized agents to gain access to consumers’ personal information. This is particularly dangerous within the context of requests to know, where fraudsters may seek to exercise CCPA requests in order to acquire sensitive information about consumers for malicious purposes, such as stalking or extortion.

W387-2
cont

CTIA therefore requests the following language be inserted into § 999.326(a):

§ 999.326(a). *When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to verify their own identity and/or provide proof that the consumer gave the agent signed permission to submit the request.*

- b. The Department should clarify that the modified regulations permit businesses to require consumers to both verify their own identity and directly confirm that they have provided the authorized agent with permission.**

Under the modified regulations, businesses are permitted to **either** (1) verify consumer’s identity, **or** (2) directly confirm with the consumer that they provided the authorized agent with permission. However, businesses are not expressly permitted to do both. Nevertheless, in many contexts, businesses may need to deploy both antifraud measures concurrently in order to effectively protect consumers.

W387-3

For example, if a business verifies a consumer’s identity, but is prohibited from further confirming that the consumer granted the agent permission to submit a request, the business is unable to adequately assess the validity of the agent’s request. Likewise, if a business verifies that an alleged “consumer” granted an agent permission but is prohibited from verifying that the “consumer” herself is who she says she is, the validity of such permission remains unclear.

Accordingly, businesses should be empowered to take **either or both** steps to adequately protect consumers, as determined by the context and sensitivity of the request.

For these reasons, CTIA requests the following language be inserted into § 999.326(a):

§ 999.326(a). . . . *The business may also require the consumer to do either or both of the following:*

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission

W387-3
cont

CONCLUSION

CTIA appreciates the Department's consideration of these comments and stands ready to provide any additional information that would be helpful.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA

1400 16th St. NW, Suite 600
Washington, DC 20036
(202) 736-3200

October 28, 2020

From: [Monticollo, Allaire](#)
To: [Privacy Regulations](#)
Cc: [Signorelli, Michael A.](#)
Subject: Joint Ad Trade Comments on Third Set of Proposed Modifications to Text of CCPA Regulations
Date: Wednesday, October 28, 2020 1:53:54 PM
Attachments: [Joint Ad Trade FINAL Comments on Third Set of Modifications to CCPA Regulations.pdf](#)

Dear Attorney General Becerra:

Please find attached joint comments from the following advertising trade associations on the content of the third set of proposed modifications to the text of the California Consumer Privacy Act regulations: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, the Digital Advertising Alliance, and the Network Advertising Initiative.

If you have any questions, please feel free to reach out to Mike Signorelli at [REDACTED] or by phone at [REDACTED].

Best Regards,
Allie Monticollo

Allaire Monticollo, Esq. | Venable LLP
t [REDACTED] | f 202.344.8300
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] | www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Third Set of Proposed Modifications to Text of California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the third set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations.¹

As explained in more detail below, the OAG's proposed modifications: (1) unreasonably restrict consumers from receiving important information about their privacy choices, (2) prescriptively describe how businesses must provide offline notices, and (3) unfairly fail to hold authorized agents to the same consumer notice standards as businesses. The OAG's potential changes to Section 999.315 would inhibit consumers from receiving transparent information and impinge on businesses' right to free speech. In addition, the proposed modifications to Section 999.326 would not provide any protections for consumers related to their communications with authorized agents, as such agents are not presently held to similar consumer notice rules as businesses. Finally, the OAG's proposed edits to Section 999.306 could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify the modifications per the below comments.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising expenditures. Locally, our members are estimated to help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.² We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous comment submissions and in the sections that follow below, the draft regulations implementing the law should be updated to better enable consumers to exercise informed choices and to help businesses in their efforts to continue to provide value to California consumers while also supporting the state's economy.³

¹ See California Department of Justice, *Notice of Third Set of Proposed Modifications to Text of Regulations* (Oct. 12, 2020), located at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-third-mod-101220.pdf?>

² IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <http://www.ana.net/getfile/23045>.

³ Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. See *Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set1.pdf> at CCPA_15DAY_000554 - 000559; *Second Set of Proposed Regulations Implementing the California*

Our members are committed to offering consumers robust privacy protections while simultaneously providing access to ad-funded news, apps, and a host of additional online services. These are offerings we have all become much more dependent on in recent months with the widespread proliferation of the COVID-19 pandemic. Ad-supported online content services have been available to consumers and will continue to be available to consumers so long as laws allow for innovation and flexibility without unnecessarily tilting the playing field away from the ad-subsidized model. The most recent modifications to the CCPA regulations set forth a prescriptive interpretation of the CCPA that could limit our members' ability to support California's employment rate and its economy in these unprecedented times. We believe a regulatory scheme that offers strong individual privacy protections and enables continued economic advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA regulations for Californians as well as the economy.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

The U.S. economy is fueled by the free flow of data. Throughout the past three decades of the commercial Internet, one driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet by delivering new, innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this responsible advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.⁴ This means that the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.⁵

W388-1

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. In a September 2020 survey conducted by the Digital Advertising Alliance, 93 percent of consumers stated that free content was important to the overall value of the Internet and more than 80 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.⁶ The survey also found that consumers estimate the personal value of ad-supported content and services on an annual basis to be \$1,403.88, representing an increase of over \$200 in value since 2016.⁷ Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored

Consumer Privacy Act, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA_2ND15DAY_00309 - 00313.

⁴ John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

⁵ *Id.*

⁶ Digital Advertising Alliance, *SurveyMonkey Survey: Consumer Value of Ad Supported Services – 2020 Update* (Sept. 28, 2020), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf.

⁷ *Id.*

experience, and research demonstrates that they are generally not reluctant to participate online due to data-driven advertising and marketing practices.

Without access to ad-supported content and online services, many consumers would be unable or unwilling to participate in the digital economy. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁸ The ad-supported Internet therefore offers individuals a tremendous resource of open access to information and online services. Without the advertising industry's support, the availability of free and low-cost vital online information repositories and services would be diminished. We provide the following comments in the spirit of preserving the ad-supported digital and offline media marketplace that has provided significant benefit to consumers while helping to design appropriate privacy safeguards to provide appropriate protections for them as well.

W388-1
cont

II. The Regulations Should Support Consumers' Awareness of the Implications of Their Privacy Decisions, Not Hinder It in Violation of the First Amendment

The proposed online and offline modifications unreasonably limit consumers' ability to access accurate and informative disclosures about business practices as they engage in the opt out process. Ultimately, this restriction on speech would not benefit consumers or advance a substantial interest. The proposed rules state: "Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request."⁹ This language unduly limits consumers from receiving important information as they submit opt out requests. It is also overly limiting in the way that businesses may communicate with consumers. As highlighted above, data-driven advertising provides consumers with immensely valuable digital content for free or low-cost, as well as critical revenue for publishers, by increasing the value of ads served to consumers. As the research cited above also confirms, consumers have continually expressed their preference for ad-supported digital content and services, rather than having to pay significant fees for a wide range of apps, websites, and internet services they use. However, as a result of the proposed modifications, consumers' receipt of factual, critical information about the nature of the ad-supported Internet would be unduly hindered, thereby undermining a consumer's ability to make an informed decision. A business should be able to effectively communicate with consumers to inform them about how and why their data is used, and the benefit that data-driven advertising provides as a critical source of revenue.

W388-2

It is no secret that consumers greatly value the information they can freely access online from digital publishers. However, local news publishers, for instance, continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising. However, the proposed modifications, as drafted, could obstruct consumers from receiving truthful, important information by hindering a business' provision of a reasonable notice to consumers about the funding challenges opt outs pose to their business model.

The CCPA regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt out process. The proposed modification would

⁸ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

⁹ Cal. Code Regs. tit 11, § 999.315(h)(3) (proposed Oct. 12, 2020).

impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet as described in Section I, and, as explained in Section III, they may be contemporaneously receiving partial or misleading negative information about their opt out rights.

To ensure a fully informed privacy choice, consumers must have every ability to access information about business practices and the benefits of the digital advertising ecosystem. Providing ample and timely opportunities for consumers to gain knowledge about their choice to opt out is of paramount importance to avoid confusion and ignorance; this allows a consumer to be fully informed about the actual implications of their decision. By prohibiting a business from requiring a consumer to “to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request” the regulations do not safeguard against this concern. As presently written, the proposed modification appears to limit businesses’ ability to provide such vital information as a consumer is opting out, even if such information is presented in a seamless way. It is unclear what amount of information, or what method in which such information is presented, could constitute a violation of the rules. Instead of setting forth prohibitive rules that could reduce the amount of information and transparency available to consumers online, the OAG should prioritize facilitating accurate and educational exchanges of information from businesses to consumers. As a result, we ask the OAG to revise the text of the proposed modification in Section 999.315(h)(3) so that businesses are permitted to describe the impacts of an opt out choice while facilitating the consumer’s request to opt out.

W388-2
cont

Additionally, the restrictions created by this proposed modification infringe on businesses’ First and Fourteenth Amendment right to commercial speech. As written, Section 999.315(h)(3) restricts the information consumers can receive from businesses as they submit opt out requests by limiting the provision of accurate and truthful information to consumers. The Supreme Court has explained that “people will perceive their own best interest if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . .”¹⁰ Because this proposed regulation prescriptively regulates channels of communication, it violates the First and Fourteenth Amendments.

The state may not suppress speech that is “neither misleading nor related to unlawful activity” unless it has a substantial interest in restricting this speech, the regulation directly advances that interest, and the regulation is narrowly tailored to serve that interest.¹¹ The proposed regulation fails each part of the test:

W388-3

- **No substantial interest:** Although there is no stated justification in the proposal, the most likely interest would be to streamline opt out requests by making it easier and faster to submit opt-outs. The OAG presumably wants nothing to impede consumers from opting out, but it is unclear because the OAG has not affirmatively stated its purpose for the proposed modification. Consumers should be made aware of the ramifications of their opt out decisions as they are opting out – not after confirming a request – so they do not make opt out choices to their detriment because they do not know the effect of such choices. For this reason, they should be able to receive information from businesses about the consequences of their opt out choices as they are submitting opt out requests. Providing information concerning the impact of an opt out is not an impediment to the process, but rather improves it.

¹⁰ *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U. S. 748, 770 (1976).

¹¹ *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980); *see also Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

- **No advancement of the interest:** If streamlining opt out requests to remove perceived impediments is the justification for the proposed rule, then the proposal does not advance that interest. The proposed regulation already includes many other specific requirements that facilitate speed and ease of opt-outs, including a requirement to use the minimal number of steps for opt-outs (and no more than the number of steps needed to opt in), prohibiting confusing wording, restricting the information collected, and prohibiting hiding the opt-out in a longer policy, all of which directly advance this interest without suppressing speech. The proposed rule limiting businesses from clicking through or listening to reasons would not make the opt out process easier for consumers, because it could result in consumers making uninformed choices if they are not notified of the consequences of their decision to opt out as they are making it. A “regulation may not be sustained if it provides only ineffective or remote support for the government’s purpose.”¹² This proposed regulation is both ineffective and provides no support for the government’s purpose.
- **Not narrowly tailored:** The proposed regulation is an overly broad and prescriptive restriction on speech that hinders accurate and educational communications to consumers about the consequences of a decision to opt-out. The regulations already include various other provisions that work to streamline the opt out process. “[I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.”¹³ As noted above, there are many ways to craft regulations to require simple and fast opt-out mechanisms that do not suppress lawful and truthful speech.

W388-3
cont

In sum, the regulation violates each and every prong of the framework for evaluating commercial speech. “As in other contexts, these standards ensure not only that the state’s interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message.”¹⁴ The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The OAG should revise the text of the proposed modification in Section 999.315(h)(3) to avoid running afoul of the First and Fourteenth Amendments and to ensure consumers may receive information about the impacts of an opt out request as they engage in the opt out process with a business.

III. The Proposed Modifications Should Impose the Same Notice Requirements on Authorized Agents as They Impose on Businesses

The proposed modifications to the CCPA regulations would require a business to ask an authorized agent for proof that a consumer gave the agent signed permission to submit a rights request.¹⁵ Although this provision helps ensure businesses can take steps to verify that authorized agents are acting on the true expressed wishes of consumers, the proposed modifications do not offer consumers sufficient protections from potential deception by authorized agents. For example, while the proposed modifications would impose additional notice obligations on businesses,¹⁶ those requirements do not extend to authorized agents. Authorized agents consequently have little to no guidelines or rules they must follow with respect to their communications with consumers, while businesses are subject to onerous, highly restrictive requirements regarding the mode and content of the information they may provide to Californians. The asymmetry between the substantial disclosure obligations for businesses and the lack thereof for authorized agents could enable (and, in fact, could incentivize) some agents to give consumers misleading

W388-4

¹² *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).

¹³ *Id.*

¹⁴ *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).

¹⁵ Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).

¹⁶ *Id.* at § 999.315(h)(3).

or incomplete information. We encourage the OAG to take steps to modify the proposed modifications to the CCPA regulations in order to equalize the notice requirements placed on businesses and agents, thus ensuring consumers can act on an informed basis under CCPA. In Section II of this submission, we discuss related First Amendment and communications fairness issues implicit in a balanced consumer privacy notice regime.

W388-4
cont

IV. Proposed Modifications to the CCPA Regulations Should Enable Flexibility in Methods of Providing Offline Notice

The proposed modifications to the CCPA regulations related to offline notices present a number of problems for consumers and businesses. As written, the CCPA implementing regulations already provide sufficient guidance to businesses regarding the provision of offline notice at the point of personal information collection in brick-and-mortar stores.¹⁷ The proposed modifications are more restrictive and prescriptive than the current plain text of the CCPA regulations, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. We therefore ask the OAG to update the proposed modifications to: (1) remove the proposed illustrative example associated with brick-and-mortar stores, and (2) explicitly enable businesses communicating with Californians by phone to direct them to an online notice where CCPA-required disclosures are made to satisfy their offline notice obligation, a medium which is more familiar to consumers for these sorts of disclosures along with having the added benefit of being able to present additional choices to the consumer.

The proposed modifications would require businesses that collect personal information when interacting with consumers offline to "provide notice by an offline method that facilitates consumers' awareness of their right to opt-out."¹⁸ The proposed modifications proceed to offer the following "illustrative examples" of ways businesses may provide such notice: through signage in an area where the personal information is collected or on the paper forms that collect personal information in a brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.¹⁹ While the illustrative examples set forth limited ways businesses can give notice in compliance with the CCPA, they are more restrictive than existing provisions of the CCPA regulations and detract from the flexibility businesses need to provide required notices that do not burden consumers or cause unreasonable friction or frustration during the consumer's interaction with the business.

W388-5

The illustrative example related to brick-and-mortar store notification sets forth redundant methods by which businesses may provide notices in offline contexts. The CCPA regulations already address such methods of providing offline notice at the point of personal information collection by stating, "[w]hen a business collects... personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online."²⁰ The proposed modifications regarding notice of the right to opt out in offline contexts are therefore unnecessary, as the regulations already address the very same methods of providing offline notice and offer sufficient clarity and flexibility to businesses in providing such notice.

In addition, the proposed modifications related to brick-and-mortar store notification are overly prescriptive. They include specific requirements about the *proximity* of the offline notice to the area where personal information is collected in a store. The specificity of these illustrative examples could result in

¹⁷ Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).

¹⁸ Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Oct. 12, 2020).

¹⁹ *Id.*

²⁰ Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).

over-notification throughout a store as well as significant costs. For example, the proposed modification could be interpreted to require signage at each cash register in a grocery store, as well as signage at the customer service desk, in the bakery area of the store where consumers can submit requests for cake deliveries, and in any other location where personal information may be collected. They also do not account for different contexts of business interactions with consumers. A business operating a food truck, for instance, would have different offline notice capabilities than an apparel store. A single displayed sign in a brick-and-mortar store, or providing a paper version of notice, would in most instances provide sufficient notice to consumers of their right to opt out under the CCPA. Bombarding consumers with physical signs at every potential point of personal information collection could be overwhelming and would ultimately not provide consumers with more awareness of their privacy rights. In fact, this strategy is more likely to create privacy notice fatigue than any meaningful increase in privacy control, thus undercutting the very goals of the CCPA.

Additionally, the proposed modifications' illustrative example of providing notice orally to consumers on the phone appears to suggest that reading the full notice aloud is the only way businesses can provide CCPA-compliant notices via telephone conversations. Reading such notice aloud to consumers would unreasonably burden the consumer's ability to interact efficiently with a business customer service representative and would likely result in consumer annoyance and frustration. Requiring businesses to keep consumers on the phone for longer than needed to address the purpose for which the consumer contacted the business would introduce unneeded friction into business-consumer relations. Instead, businesses should be permitted to direct a consumer to an online link where information about the right to opt out is posted rather than provide an oral catalog of information associated with particular individual rights under the CCPA.

The proposed modifications' addition of illustrative examples regarding methods of offline notice is unnecessary, redundant, and inflexible. These modifications would result in consumer confusion, leave businesses wondering if they may take other approaches to offline notices, and if so, how they may provide such notice within the strictures of the CCPA. We therefore ask the OAG to remove the proposed illustrative example associated with brick-and mortar stores as well as clarify that businesses communicating with consumers via telephone may direct them to an online website containing the required opt out notice as an acceptable way of communicating the right to opt out.

* * *

W388-5
cont

Thank you for the opportunity to submit input on the content of the proposed modifications to the CCPA regulations. Please contact Mike Signorelli of Venable LLP at [REDACTED] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance

From: [Paul Jurcys](#)
To: [Privacy Regulations](#)
Cc: [Admin Prifina](#); [Markus Lampinen](#)
Subject: Prifina"s Comments to CCPA Regulations
Date: Wednesday, October 28, 2020 3:01:39 PM
Attachments: [CCPA-Prifina"s comments #3.pdf](#)

Dear Ms. Kim,

Please find Prifina's comments.

Sincerely,

Paul

--

Paul Jurcys, LL.M. (Harvard), Ph.D.
Co-Founder | [Prifina](#)
1 Market St., San Francisco

**Dr. Paul Juncys and
Markus Lampinen**

**1 Market Street
Spear Tower, Suite 3600
San Francisco, CA 94105
policy@prifina.com**

October 28, 2020

Lisa B. Kim,
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

**Prifina's Comments to the OAG's proposed Third Set of
Modifications of the CCPA Regulations**

Dear Ms. Lisa B. Kim,

Prifina Inc. is pleased to have the opportunity to provide its responses to the text of modified CCPA Regulations. We would like to thank the Office of the Attorney General for making it possible for various interested parties to express their views on this significant piece of legislation. We admire that the office of the Attorney General has taken a firm stance to protect consumers' rights related to data privacy and ensuring that those rights are given priority in building a more fair and balanced digital market.

We hope that our comments will contribute to the improvement of the legal framework governing data privacy in California.

Sincerely yours,

Paul Juncys and Markus Lampinen

Prifina's Comments to the OAG's proposed Third Set of Modifications of the CCPA Regulations

October 28, 2020

Prifina believes that data privacy is a fundamental human right and we would like to congratulate the Office of the Attorney General for all the hard work that is being done to create a legal environment for more equitable and transparent use of an individuals' personal data. At Prifina, we believe that individual consumers should not only have rights to their data held by third parties but also be able to get value from their personal data. To realize this, we are building tools that help individuals have "master copies" of their personal data, as well as tools for developers to build new types of applications that run on top of the user-held data.

Prifina generally agrees with the most recent proposals to amend the CCPA Regulations and welcomes the OAG's efforts to gather opinions from various stakeholders. In many instances, compliance with the CCPA requires balancing four sets of considerations: data and technology architecture, legal, user experience and interface and numerous issues related to user behavior and psychology. In the following paragraphs, we will provide some insights and suggestions on issues that need to be taken into consideration while improving the text of the Regulations and to facilitate effective implementation.

1. Providing Notices to Opt-Out of Sales of Data (S. 999.306(b)(3))

Providing notices about the possibility of a consumer to opt-out from sales of personal data often depends on the actual circumstances when the data is collected from the consumer. From a practical perspective, it may be questioned what interactions with consumers could be deemed as "offline". For instance, offline interactions in most cases involve collecting data in various formats: making payments via a credit card, offering consumers the ability to check-in by filling in forms on a tablet, signing waivers or having a security camera on the premises of a business already means that data about consumers is being collected. Most businesses also have websites in which customers can be notified about their terms of use, privacy and data collection policies.

Section 999.306(b)(3)(a). With regard to brick and mortar businesses, such as theme parks or locations providing physical services, the notification about the opportunity to opt out from sales of personal information could be done at three different instances.

W389-1

First, information about the possibility to opt-out from sales of data can be provided at the point of entry into a business by placing a notice or an icon displaying data collection practices of the business. Such a notice could be a simple set of words (e.g., “we do not collect your data”, “we do not sell your data” or “we sell your biometric data, ask our staff how to opt-out”, etc.). It is quite possible that businesses could start using certain visual icons to communicate with the consumer about the data collection practices at a given location. At the moment when this comment is submitted, there are no uniform privacy icons to visualize businesses’ data collection and usage practices and communicate them clearly to consumers. However, some businesses as well as researchers have been working on different initiatives to develop icons for data disclosures.¹

In this regard, the OAG may consider what possible steps it should take to facilitate the creation of icons for data collection and data use and how to ascertain that those data disclosures are easily understandable from an average consumer perspective. The OAG may consider collaborating with businesses and researchers. The OAG may also create a more formal study group consisting of representatives of businesses, academics, researchers, legal experts and designers to develop examples of icons that can be used to communicate consumer options with regard to their personal data. Such icons for data disclosures could be a powerful tool in promoting consumer data literacy both in brick-and-mortar as well as online interactions.

W389-1
cont

The second instance where notices about the right to opt-out from the sales of data occurs is at the time when the individual consumer has either to sign a waiver (before entering a facility) or making a payment. Again, notifications about the right to opt-out can be made by placing a data disclosure icon, displaying a text message (with or without accompanying instructions), placing a bar code which would lead the consumer who scans the code with her hand-held device to the website where the procedure for opt-out can be completed or by simply checking the box that could mark consumers’ preference to opt-out from the sales of data.

Third, notices about opting out from the sales of data could also be made after visiting brick-and-mortar facility. Provided that the business has the consumer’s contact information (physical address, email address or cell phone number), the business could send instructions on how to opt-out from the sales of data. Similar practices are currently employed by various institutions that offer financial services. Consumers are periodically (usually at the beginning of the year) sent notices about the possibility of opting out of sales of their data.

¹ See e.g., Paulius Juncys “Privacy Icons and Legal Design”, available at: <https://towardsdatascience.com/privacy-icons-4ca999a6f2db>, and Zohar Efroni, Jakob Metzger, Lena Mischau, and Marie Schirmbeck, “Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing” (2019) EDPL Vol. 5, p. 352, available at: <https://edpl.lexxion.eu/article/EDPL/2019/3/9>.

From the consumer’s point of view, however, the notices about data collection practices and the right to opt-out could become quite disturbing. As a matter of fact, nowadays security camera icons are displayed in almost every shop or venue. Time will show whether the customers’ experience and emotions will be affected by notices that their data is being collected, shared with third parties and that they have the right to opt-out. Furthermore, filling in the form before, during or after the experience might be quite time-consuming and contribute to notice fatigue. It may also be questioned whether such a communication about the right to opt-out would be effective (i.e., whether consumers will actually exercise such an option).

W389-1
cont

Section 999.306(b)(3)(b). Similar to brick-and-mortar situations, notifications about the right to opt-out from sales when the interaction with the consumer takes place via the phone is based on the assumption that the business already has some data (at least contact information) about the consumer. Currently, many phone calls are recorded which adds another layer of consideration about how that data is being used and exactly what notices about the right to opt-out from sales should contain. Given California already requires explicit consent of all parties before a call is recorded, a disclosure to opt-out in the same situation may be logical.

From a consumer psychology point of view, notices about the right to opt-out from sales of data are complex. Such notices to opt-out might put the consumer in an uncomfortable position because the consumer may be forced to say something she may not not be comfortable saying in a verbal conversation or that may be perceived to lessen the service she receives. Hence, the OAG might want to consider whether businesses who are collecting and selling consumer data should be required to provide the consumer with directions on how to opt-out from the sales of data after the phone call.

W389-2

It appears that that Section 999.306(b)(3)(b) is incomplete and should be clarified as follows (our suggestion is highlighted in yellow):

- b. A business that collects personal information over the phone may provide the notice orally during the call what information is collected and sold, and explain to the consumers how to opt-out of sales after the call is over.**

2. Requests to Opt-Out (S. 999.315(h))

Prifina believes that offering illustrative examples of practices that businesses should not employ is certainly helpful. Generally speaking, while examples provided in Section 999.315(h) are relevant today, one might wonder if the illustrative list would still be meaningful tomorrow?

W389-3

Accordingly, it would be reasonable for the OAG to follow the emerging CCPA compliance practices and regularly update the prohibited practices that hinder the consumers' opportunity to opt-out from sales of data.

More specifically, Prifina has noticed that businesses tend to require consumers to provide additional information which is justified by the need to verify the identity of the requestor. We have noticed that in some instances, the verification process ends-up being quite time-consuming and involves multiple steps. This proves to be quite a cumbersome experience for consumers. In practical terms, businesses need to find more efficient ways to structure their data and establish record-keeping practices. To facilitate this, the OAG could provide some non-binding guidelines and recommendations to help businesses transition to more efficient data practices.

W389-3
cont

3. Authorized Agents (S. 999.326(a))

Prifina welcomes the proposed modifications to Section 999.326(a) because they should contribute to making consumer interactions with businesses via authorized agents more smooth. It should be recalled that one of the main incentives for consumers to employ authorized agents is the willingness to reduce the burden and hassle related to dealing with third parties that process consumer's personal information. In practice, balancing security, fraud prevention, transparency and efficiency of communication can be quite challenging. Therefore, the deletion of the possibility for businesses to require authorized agents to provide written permission of the consumer is definitely a positive step forward. The regulator should seek to create an environment where consumer interactions via an authorized agent are frictionless.

W389-4

Nevertheless, the current version Section 999.326(a) leaves an ample spectrum of possibilities for businesses to delay the fulfillment of requests submitted via an authorized agent, by adding an additional verification step. The possibility which businesses now have to ask the consumer to verify the consumer's identity or confirm that they have authorized the agent to act on their behalf opens the gate for double verification. This could have quite an adverse effect on consumers because the whole point of using authorized agents is to streamline the opt-out process and avoid multiple verifications that are employed by businesses on a case-by-case basis.

W389-5

More particularly, the consumer's "signed permission to submit request", in principle, should be deemed sufficient unless there are some reasonable grounds to believe otherwise. One possible solution to resolve such an information asymmetry is to create an industry-wide template of a signed permission which should be deemed sufficient for the business to comply

W389-6

with the request submitted via an authorized agent. This **signed permission template** could be prepared by the OAG (which could then cooperate with industry and consumer representatives). This would help find balance between different regulatory objectives, save time, cost, and would reduce information asymmetries between all parties involved.

W389-6
cont

In situations where a consumer interacts with businesses via an authorized agent, it is desirable that businesses have a **designated point of contact** with whom authorized agents should be able to interact with. This would facilitate the interaction between the authorized agent and businesses.

W389-7

Finally, if the AOG decides to keep the proposed structure of Section 999.326(a), we would like to suggest narrowing down the scope of subsections (1) and (2) by adding an additional qualifier which would allow businesses to contact the consumer in cases where the authorized agent has not provided **reasonable proof** of the existence of the signed mandate.

W389-8

4. The Wording of S. 999.332(a)

We recommend deleting “and” and keeping the text of Section 999.332(a) as following:

§ 999.332. Notices to Consumers Under 16 Years of Age.

- (a) A business subject to sections 999.330 ~~and~~or 999.331 shall include a description of the processes set forth in those sections in its privacy policy.

W389-9

From: [Courtney Jensen](#)
To: [Privacy Regulations](#)
Subject: TechNet Comment Letter Regarding Third Set of Proposed Modifications to CCPA Regulations
Date: Wednesday, October 28, 2020 3:20:03 PM
Attachments: [TechNet CCPA Regulation Letter 10.28.20.pdf](#)

Good Afternoon,

Attached please find TechNet's written comments regarding the third set of proposed modifications to CCPA regulations.

Please do not hesitate to reach out with any questions.

Thank you,
Courtney

Courtney Jensen
Executive Director | California and the Southwest
TechNet | The Voice of the Innovation Economy





October 28, 2020

The Honorable Xavier Becerra
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Dear Mr. Attorney General Becerra,

TechNet appreciates the opportunity to submit written comments regarding the third set of proposed modifications to the California Consumer Privacy Act (“CCPA”) regulations.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet’s diverse membership includes dynamic startups and the most iconic companies on the planet and represents three million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet member companies place a high priority on consumer privacy. We appreciate the aim of the CCPA to meaningfully enhance data privacy; however, we continue to be concerned that CCPA regulations are not finalized and it is not clear when these new draft regulations would be final and implemented. This raises significant compliance problems for a law that took effect January 1, 2020 and for which enforcement began July 1, 2020. We believe these modifications should include language making the changes effective six months to one year from publication of final regulations. This will give businesses the opportunity to properly implement complex regulations for a complex law. This implementation time is especially important during the ongoing COVID-19 crisis where personnel are working remotely and businesses are continuing to recover from services being shut down.

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information.

- For opt-out notices in an offline setting such as a retail store, TechNet believes that such a notice should only be required if information collected in that offline setting or from an offline transaction is sold, consistent with the rest of CCPA.

W390-1

§ 999.315 Requests to Opt-Out.

- TechNet has concerns with h(3) and h(4) as outlined in the modified regulations and the vagueness, lack of detail and compelled speech these sections present.

- o (h)(3) states *"Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to optout before confirming their request."* This illustrative examples ties the hands of companies to provide additional information to their consumers. Companies would not be able to provide more disclosures or information that could explain to consumer the implications of their decisions. This does not further the intent of the CCPA which is to promote consumer transparency and information. For example, during an opt out process a business may include information that explains what a data sale is and the impact of opting out. This would not be allowed under (h)(3). We believe providing this information stays true to the spirit of CCPA and simply educates consumers. We believe (h)(3) is especially unnecessary with the inclusion of (h)(1) which ensures ease for consumers. Businesses should be able to explain the impacts and/or drawbacks of opting out, since many consumers may not understand what it means. W390-2
- o (h)(4) states *"The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request."* We are concerned with the vagueness and lack of detail given for the new illustrated example. If this new example is to be added, then businesses need more guidance as to what personal information is actually needed versus what is not needed to avoid confusion for both businesses and California resident "consumers." W390-3

Conclusion

TechNet thanks you for taking the time to consider our comments on the proposed modifications to the CCPA regulations. We again urge that any new proposed modifications give businesses proper time to come into compliance with the regulations. Our goal for all CCPA regulations is that they should help facilitate compliance on the part of California businesses, while ensuring that consumers have the information necessary for them to make informed decisions regarding their rights under the CCPA.

If you have any questions regarding this comment letter, please contact Courtney Jensen, Executive Director, at [REDACTED] or [REDACTED].

Thank you,
Courtney Jensen
Executive Director, California and the Southwest
TechNet

From: [Dylan Hoffman](#)
To: [Privacy Regulations](#)
Subject: Internet Association Comments on Third Modified CCPA Regulations
Date: Wednesday, October 28, 2020 3:53:05 PM
Attachments: [IA Comments on Proposed Modified Regulations to CCPA 10.28.20 \(1\).pdf](#)

Hi,

Please find attached comments from Internet Association on the Third Modified CCPA Regulations. If you have any questions please let me know.

Best,

--



Dylan Hoffman

Director of California Government Affairs



INTERNET ASSOCIATION

1303 J Street, Suite 400, Sacramento, CA 95814



Check out [Internet Association's job site](#) with hundreds of internet industry positions now open!



October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Internet Association (“IA”) appreciates the opportunity to review and provide the Attorney General’s Office (“AGO”) feedback on the Text of Modified Regulations for the California Consumer Privacy Act (“CCPA”) Regulations (“Modified Regulations”). IA is the only trade association that exclusively represents leading global internet companies on matters of public policy.¹ Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society, and as the voice of the world’s leading internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits. IA members are committed to providing consumers with strong privacy protections and control over personal information, as well as to compliance with applicable laws, and advocates for a modern privacy framework in the IA Privacy Principles.² Internet companies believe individuals should have the ability to access, correct, delete, and download data they provide to companies both online and offline.

IA hopes to continue working with the AGO to clarify these regulations. We are encouraged by some of the recent proposals in the latest Modified Regulations, but have some constructive feedback around certain provisions within the proposed language.

IA COMMENTS

General

IA member companies are concerned about the continuous nature of the CCPA regulations process. We appreciate the AGO doing its part to protect consumers and clarify or provide guidance for some of the confusing language within the CCPA. However, adding new requirements, as these modifications do, makes compliance more difficult for businesses and impacts consumers’ abilities to exercise their rights under the law. While we are supportive of the AGO’s goal to provide greater clarity, closing the door on the rulemaking process for a period of time will allow businesses to implement the current regulations and regulators to identify the true challenges within the new rules.

W391-1

999.315 (h)

- **Section 999.315 (h)(1-5)**

- These sections are intended to provide illustrative examples of how businesses should make requests to opt-out easy for consumers to execute. While the examples are intended to provide clarity, they are framed in a statutory “shall not” form, implying that businesses must comply

W391-2

¹ IA’s full list of members is available at: <https://internetassociation.org/our-members/>.

² IA Privacy Principles for a Modern National Regulatory Framework, available at: https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_fulldoc / (last accessed November 25, 2019).



with their prescriptions.

- IA would recommend the following suggestions below that are inspired by the six verification considerations set forth in section 999.323 (b)(3). Under the aforementioned section, the regulations present the format of a consideration and how a business should apply that consideration. Using this format provides businesses with greater clarity and guidance about how to design and process consumer requests to opt-out.

W391-2
cont

● (h)(3)

- IA member companies are concerned about the current language of (h)(3) limiting businesses' ability to provide more transparency to consumers. As currently drafted, this subsection could potentially inhibit companies from providing additional context and information to consumers about how they protect and use consumer data. We would recommend that the AGO review this language and IA's recommendations below to provide consumers with the ability to fully understand the implications of choosing to opt-out prior to making their decision.

W391-3

- Furthermore, IA is concerned that (h)(3) may raise compelled speech issues, as it would prohibit companies from providing consumers with additional information about the implications of their opt-out.

W391-4

- IA member companies would encourage the AGO to consider adopting a reasonableness standard, as noted below, for what information companies can provide to consumers during the opt-out decision process. Our companies would like to supply pertinent and reasonable information to consumers to help them make informed decisions about the use of their personal information.

W391-5

○ **IA Suggested Text Alterations:**

- (h) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose ~~or has the substantial effect~~ of subverting or impairing a consumer's choice to opt-out. A business shall consider the following factors when creating processes for requests to opt-out: ~~Illustrative examples follow:~~

- (1) The number of steps included in t~~he~~ business's process for submitting a request to opt-out as compared to the number of steps included in the~~shall not require more steps than that~~ business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out ~~should be~~is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information ~~should be~~is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request. The number of steps included in the business's process for submitting a request to opt-out should not unreasonably exceed the number of steps included in the business's process for a consumer to opt-in to the sale of personal information after having previously opted out.

W391-2
through
W391-5



- (2) Whether the business uses ~~A business shall not use~~ confusing language, such as double-negatives (e.g., “Don’t Not Sell My Personal Information”), when providing consumers the choice to opt-out. The business should avoid using confusing language such as double-negatives.
- (3) Whether a business unreasonably requires ~~Except as permitted by these regulations, a business shall not require~~ consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request. The business should avoid unreasonably requiring consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request, except as permitted by these regulations.
- (4) Whether t~~The business’s~~ process for submitting a request to opt-out ~~shall not~~ requires the consumer to provide personal information that is not necessary to implement the request. The business should avoid requiring consumers to provide personal information that is not necessary to implement the request to opt-out.
- (5) Whether, u~~Upon~~ clicking the “Do Not Sell My Personal Information” link, the business ~~shall not~~ requires the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out. The business should avoid requiring consumers to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.

W391-2
through
W391-5
cont

Respectfully,

Dylan Hoffman
Director of California Government Affairs
Internet Association

From: [Jen King](#)
To: [Privacy Regulations](#)
Cc: [Adriana Stephan](#)
Subject: Re: CCPA comments for 10/29/20 rulemaking
Date: Monday, November 2, 2020 11:20:43 AM
Attachments: [CCPA comments October 28 2020 corrected.pdf](#)

Greetings,

I realized after submitting our comments last week that the version I sent in was missing our footnotes. Attached is an updated version (the only changes are the inclusion of footnotes that should have been in the submitted copy!). Please let me know if you are able to replace our existing submission with this one.

Sincerely,
Jen King

Jennifer King, Ph.D (she/her)
Director of Consumer Privacy
Center for Internet and Society
Stanford Law School

<https://cyberlaw.stanford.edu/about/people/jen-king>

www.jenking.net/publications

Google Scholar profile: <https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en>

On Oct 28, 2020, at 4:02 PM, Privacy Regulations
<PrivacyRegulations@doj.ca.gov> wrote:

Thank you for submitting a public comment on the CCPA proposed regulations. Your email has been received.

Sincerely,
California Department of Justice

From: Jennifer King [REDACTED]
Sent: Wednesday, October 28, 2020 3:55 PM
To: Privacy Regulations <PrivacyRegulations@doj.ca.gov>
Cc: Adriana Stephan [REDACTED]
Subject: CCPA comments for 10/29/20 rulemaking

Dear Ms. Kim,

Attached please find our comments regarding the

latest revisions to the CCPA.

Best,
Jen King

Jennifer King, Ph.D

Director of Consumer Privacy - Center for Internet and Society

Stanford Law School



<https://cyberlaw.stanford.edu/about/people/jen-king>

www.jenking.net/publications

Google Scholar profile: <https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en>

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

October 28, 2020

To Whom It May Concern:

We are pleased to submit comments to the California Attorney General's office regarding the Third Set of Proposed Modifications to CCPA Regulations released on October 12, 2020. We make these comments on behalf of ourselves individually and provide our institutional affiliation for identification purposes only.

W392-1

In sum, we are heartened by the OAG's decision to further clarify §999.315 - Requests to Opt-Out. From our own experience conducting empirical research on the implementation of "Do Not Sell My Personal Information" links across a variety of websites, we observed a wide discrepancy in how individual companies have implemented this process. We found evidence of so-called "dark patterns"—as defined in Proposition 24, "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice." Whether intentionally designed to thwart Californians' exercise of their Do Not Sell right, or as a result of poor design choices, the end result is the same: unfair barriers to completing these requests. While these design choices may negatively impact all California consumers, they may have disproportionate impacts on vulnerable individuals, such as the elderly, non-English speakers, and individuals with lower written literacy and technology experience.

Our research group reviewed the Do Not Sell (DNS) processes of dozens of websites across a variety of different business types, including: brick and mortar retail stores, car dealerships, theme parks, grocery stores, pharmacies, banks, and newspapers. We observed the following problems, of which we include examples in the attached appendix:

- Do Not Sell flows (the steps by which a consumer initiates a Do Not Sell request up to completion) that included unnecessary steps for making a DNS request, such as:
 - Sending consumers from the DNS link on a company's homepage to the company's privacy policy page (or other indirect routes), rather than directly to a DNS form, thus requiring consumers to hunt through the policy to find the link to the DNS form (see Appendix 1 for an example);
 - Requiring consumers to select a button or toggle embedded within a page to make a request, often without instructions or clear labels, such that it is unclear which option initiates the DNS state (see Appendix 2 for examples);
- DNS forms that asked consumers to provide personal information that appeared extraneous to the DNS request;

- Forms offered only in English by companies that likely have large non-English speaking customer bases (see Appendix 3 for an example);
- DNS landing pages and/or forms that used confusing (e.g., double negatives) or manipulative language (e.g. emotionally charged or guilt-inducing) that attempts to persuade consumers not to exercise their rights (see Appendix 4 for an example);
- DNS landing pages that included copious amounts of text preceding the form that was not directly salient to making a request. Forcing consumers to spend additional time or energy to read extraneous information may decrease the likelihood of completing a DNS request (see Appendix 5 for an example);
- For companies that honor DNS requests only via email, many of these companies provided little or no instruction to consumers about how to complete the request (e.g., what information to include in an email), did not offer automated shortcuts for composing emails (e.g., mailto functionality that can prepopulate an email with the address and subject link when clicked), and provided email addresses that appeared to be non-specific to DNS requests, which may increase the burden on the consumer to engage in continual back-and-forth with the company to make the DNS request.

Consumer Reports, which released a report on October 1st, 2020 entitled “California Consumer Protection Act: Are Consumers’ Digital Rights Protected,” also found many of the same issues we report here, as well as additional concerns.¹

We are pleased to see the OAG address some of the issues above with additional clarifications to the statute in order to improve what should be a simple and straightforward process for consumers. These clarifications make it less onerous for both consumers to exercise their rights and for companies to comply with the CCPA. By reducing the gray area that forces companies to rely heavily on interpretation, the updated regulations diminish the potential for DNS processes to be designed in ways that are confusing, deceptive, or manipulative to consumers, whether deliberately or by accident.

At the same time, while the clarifications reduce company discretion in designing DNS processes, the current OAG guidelines still leave room for companies to implement DNS processes in ways that subvert consumers’ ability to exercise their rights under the statute.

We would like to see companies and/or policymakers also address the following:

1. Provide forms, rather than email addresses, for consumers to make DNS requests

W392-2

DNS requests that require consumers to send an email, without outlining the information consumers must provide for the request to be fulfilled, are particularly burdensome on consumers.

2. Offer DNS forms in languages other than English, and also use simple, easy to understand language

W392-3

Non-English speakers are particularly vulnerable to confusing or misleading language in DNS requests. For businesses that provide essential services and/or have a substantial non-English speaking clientele, company DNS forms should accommodate different languages (see Appendix 3 for examples of English-only privacy policies for companies with large non-English speaking customer populations).

¹ Available at: https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

3. Avoid crowding DNS forms with extraneous information

DNS forms are not the place for companies to produce treatises on why they think they do not sell information. And while providing references to useful background information on the CCPA may be helpful to consumers (including links to official guidance from the OAG's CCPA website), reproducing hundreds of words of text that is not required reading for exercising one's DNS rights is not helpful and discourages consumers from completing their requests.

W392-5

4. Provide consumers a streamlined form that does not require them to take extraneous steps to complete a DNS request. For multiple-purpose forms (e.g. forms allowing consumers to also exercise their deletion and access rights), make the selection choices simple and clear.

5. Absent a mandate to respect Global Privacy Control signals, provide a standardized interface for consumers to exercise their DNS rights.

W392-6

The CCPA presently requires companies to provide “two or more designated methods for submitting requests to opt-out.”² The vast majority of companies have elected not to adopt mechanisms such as the Global Privacy Control³, which would provide a simple and straightforward means for consumers to communicate DNS preferences with all websites they visit using a browser plug-in or setting. Unfortunately, the original requirement of the statute to develop “a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information” (§1798.185(4)(C)) was dropped during the review period. While we filed comments in February 2020 urging that the Attorney General (OAG) not adopt the version of the button proposed at that time, we did support the OAG following the advice of the CMU report to create a standardized control.⁴ Unfortunately, our research demonstrates that absent a standardized control mechanism, companies are using inconsistent and in some cases, unclear and misleading methods to allow consumers to exercise their DNS rights. Further, executing DNS requests for even a single website requires consumers to repeat these steps using every browser on every device (including mobile devices) they have used to access the website in order to fully ensure that a single company honors their DNS preference. This is, on a practical level, unworkable for consumers, and illustrates the unreasonable burden consumers must shoulder to exercise their CCPA rights.

Accordingly, we urge California policymakers to mandate the adoption of the Global Privacy Control standard. In the CCPA, §999.315(c) mandates that businesses treat “user-enabled global privacy controls, such as browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request.” The current “process” for making DNS requests on websites where cookies, rather than a user account, are the basis by which consumers are tracked is, as we note above, is highly complicated and likely deeply confusing for most consumers (Please see Appendix 6 for examples.) As the attached examples demonstrate, consumers are expected to either submit opt-out requests on each browser and device they use to visit a company’s website, or are asked to allow the site to place a cookie in order to provide a DNS signal (which becomes obsolete if a consumer elects to clear her browser cookies).

The Global Privacy Control could provide consumers with a delegated means of seamlessly providing DNS requests to companies without having to engage in the burden of making independent DNS requests for each

² §999.315(a)

³ <https://globalprivacycontrol.org/>

⁴ [Cranor, et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* \(February 4, 2020\).](#)

website they visit and on each browser and device they use. However, as we note above, businesses can refuse to honor a consumer's privacy-specific preferences if the preferences were set in the software, such as the legacy "Do Not Track" option in web browsers. As of right now, California law dictates that companies must disclose whether they respond to "Do Not Track" requests, ultimately giving them the discretion as to whether or not to honor these requests from consumers.

In closing, while we believe the §999.315 clarifications are a positive development for consumers hoping to exercise their rights under the CCPA, there are still several measures companies should take to ensure that they are not actively undermining DNS processes, particularly for vulnerable populations.

Sincerely,

Jennifer King, Ph.D
Director of Consumer Privacy
Center for Internet and Society, Stanford Law School

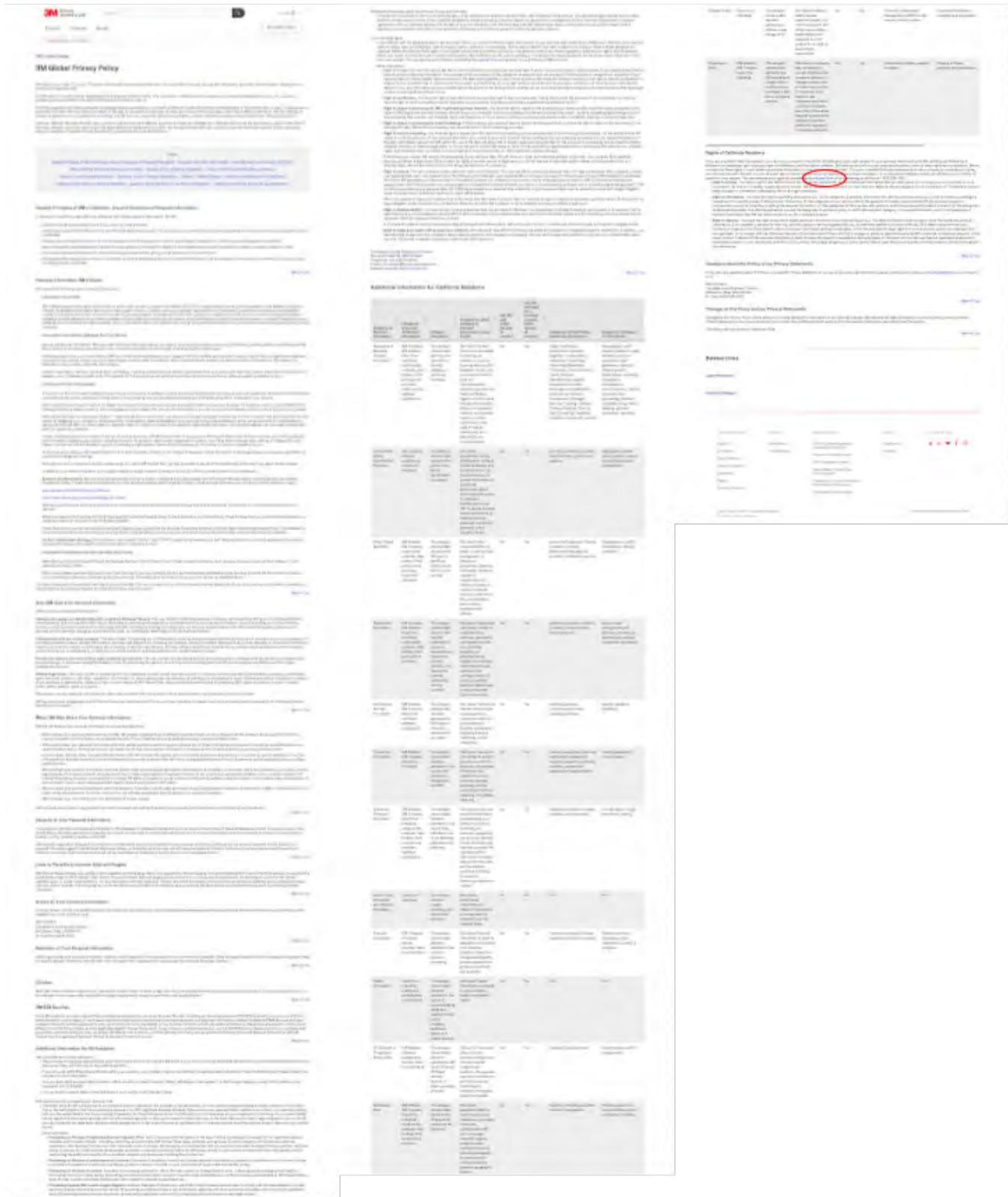
Adriana Stephan
M.A. Student
Cyber Policy, Stanford University

Emilia Porubcin and Claudia Bobadilla
Undergraduate Students, Stanford University

Morgan Livingston
Undergraduate Student, University of California, Berkeley

Appendix 1: 3M Company (https://www.3m.com/3M/en_US/company-us/privacy-policy/), visited 10/26/20

Please note that there is no "Do Not Sell" link from the homepage; this page is accessed via the privacy policy link in the footer. Due to the length of this page we have cut it into smaller sections in order to fit it all one printed page. The link in the red circle is the link to the DNS form.



Appendix 2: Examples of unclear or confusing DNS toggles or buttons

These examples illustrate how companies are using a specific form of interaction design (toggle switches) that neither clearly communicates to consumers what toggling the switch will accomplish, nor whether they have successfully opted out or not. The LA Times (Example 1) is slightly clearer than Examples 2 and 3 given that the switch is grey when arriving at the page (indicating “off”), and when clicked turns green (indicating “on”), as well as providing a “Save” button to confirm the selection. Even so, there are no instructions to follow nor text indicating the switch state. Example 2 offers consumers the choice to “agree” or “disagree”, but with what exactly is unclear (are you agreeing to opt-out? Or not?). Example 3 provides no instruction of what will occur when the toggle is switched; the consumer must deduce that the existing state (blue, presumably “on”) means that one’s data is being sold to third parties, and that toggling it to grey (“off”) will stop the sale.

Example 1: Los Angeles Times (visited 10/26/20)

Opt-Out Tools

To unsubscribe from Los Angeles Times marketing messages, you can adjust your settings here:
<https://membership.latimes.com/settings>.

If you are a California resident, to opt out of the sale of your personal information (and as a result, opt out of personalized advertising), **you must utilize the following toggle (and all 3 tools below)**.

Do Not Sell My Info

Save

If you are logged into your Los Angeles Times account, this setting will save your opt out preference to your profile (otherwise your preference will be stored in a browser cookie). Please see the [full disclosure](#) below.

You must utilize each of the following 3 tools (in addition to the toggle above) to ensure that you are opted out as much as technically possible across the open web.

1. DAA: <http://optout.aboutads.info/>
This tool, created by the Digital Advertising Alliance, will generate a list of participating vendors who are currently collecting data from you for the purposes of targeted advertising. You will be able to see each vendor and must then affirmatively opt out of any or all of their databases.
2. NAI: <http://optout.networkadvertising.org/>
This tool, created by the Network Advertising Initiative, will also generate a list of participating vendors who are currently collecting data from you for the purposes of targeted advertising. You will be able to see each vendor and must then affirmatively opt out of any or all of their databases.
3. LiveIntent: <http://d.liadm.com/opt-out>
This tool is specific to LiveIntent, which is a vendor we utilize for advertising within our newsletters.

Full disclosure: For many of these tools, your opt-out preferences may be stored in cookies. If your browser blocks cookies, your opt-out preferences may not be effective. If you delete cookies, you may also be deleting your opt-out preferences, so you should visit these pages periodically to review your preferences or to update your choices. The above opt-out mechanisms are browser based and device specific; thus, you must opt-out on each device and on each browser to exercise your rights. The Los Angeles Times does not maintain or control the opt-out mechanisms listed in items 1-3 above and is not responsible for their operation.

Example 2: Huffington Post/Verizon Media (visited 10/27/20)

The screenshot shows a consent dialog with the Huffington Post logo at the top left. A back arrow is visible on the left side. The main heading is "Continue Sharing under California Law". To the right of the heading is a toggle switch currently set to "Agree", with "Disagree" and "Agree" labels. The body text explains that Verizon Media does not sell identifying information but shares other identifiers with partners for product, service, and advertising purposes. It notes that under the California Consumer Privacy Act, some of this sharing may be considered a "sale" and that users have the right to opt out. It states that opting out will stop the sharing of data as described, which may impact services and content. A "Learn More" link is provided at the end of the text.

W392-1
cont

Example 3: CNN.Com/Warner Media (visited 10/27/20)

WarnerMedia



Do Not Sell My Personal Information

For California Residents Only
Pursuant to the California Consumer Privacy Act (CCPA)

The WarnerMedia family of brands uses data collected from this site to improve and analyze its functionality and to tailor products, services, ads, and offers to your interests. Occasionally, we do this with help from third parties using cookies and tracking technologies.

We respect your right to privacy, and we have built tools to allow you to control sharing of your data with third parties. You can choose to disable some types of cookies and opt to stop sharing your information with third parties, unless it is necessary to the functioning of the website. Click on the different category headings to find out more and to opt-out of this type of data sharing. Note that any choice you make here will only affect this website on this browser and device.

To learn more about how your data is shared and for more options, including ways to opt-out across other WarnerMedia properties, please visit the Privacy Center.

Manage Consent Preferences

Share my Data with 3rd Parties



For California Residents Only

Pursuant to the California Consumer Privacy Act (CCPA)

Some of your data collected from this site is used to help create better, more personalized products and services and to send ads and offers tailored to your interests. Occasionally this is done with help from third parties. We understand if you'd rather us not share your information and respect your right to disable this sharing of your data with third parties for this browser, device, and property. If you turn this off, you will not receive personalized ads, but you will still receive ads. Note that any choice you make here will only affect this website on this browser and device.

W392-1
cont

Appendix 3: Examples of English-only privacy policies for companies with large non-English speaking customer populations

99 Ranch Market (<https://www.99ranch.com/zh-hans/privacy-policy>), visited 10/26/20

Please note this site does not have a Do Not Sell link on the homepage; this page is accessed via the Privacy Policy link (also only in English), though the site offers an option to set the language to Chinese (simplified or traditional). In this example, the language was set to Chinese (simplified). Please note: this screenshot includes only the top portion of the webpage

The screenshot shows the top navigation bar of the 99 Ranch Market website. At the top right, there is a welcome message: "Welcome, you can sign in or create an account." followed by "My Store: Select Store" and "My Favs" with a heart icon. On the left is the 99 Ranch Market logo. Below the logo is a "Reorder" button with a circular arrow icon. Next to it is a green "All" button with a dropdown arrow. To the right is a search bar with a magnifying glass icon and the text "Search ...". Further right is a shopping cart icon with a "0" next to it. Below the search bar and cart icon is a horizontal menu with four items: "我的选店" (My Store) with a dropdown arrow, "每周特价" (Weekly Specials), "资讯/活动" (News/Events), and "关于我们" (About Us) with a dropdown arrow.

Privacy Policy

Tawa Supermarket, Inc. and our affiliates are committed to protecting your privacy. We recognize that privacy is an important issues for our customers and employees and we want to be transparent about how we collect, use, and disclose your personal information—this Privacy Notice provides you with notice of our processing activities and your rights under the law. Personal Information generally means any information that identifies you as an individual person, along with other information we associate with it. This includes information that is maintained by us in a manner that identifies you or your household. Personal information does not include publicly available information or information that is de-identified or aggregate consumer information.

By using any of our websites and mobile applications in the United States (collectively, "Sites") or otherwise providing Personal Information to us, you agree to this Privacy Policy. This Privacy Notice is intended for individuals in the United States who are over the age of 16. If you live outside of the United States and choose to use the Sites connected with this Privacy Notice, you do so at your own risk and understand that your information will be sent to and stored in the United States.

Application

This Privacy Notice applies to Tawa Supermarket, Inc., Tawa Inc. (Retail), Tawa Services, Inc., Welcome Market, Inc., Welcome California Market, Inc., and Welcome Services, Inc.

Appendix 4: Examples of websites using “guilt-shaming” or other coercive language in their DNS requests.

Example 1: BuzzFeed.com (visited 10.27/20)

Please note the text on the opt-out button: “this action will make it harder to us [sic] to tailor content for you.”

BuzzFeed - Do Not Sell My Personal Information

We, and our partners, use technologies to process personal information, including IP addresses, pseudonymous identifiers associated with cookies, and in some cases mobile ad IDs. This information is processed to personalize content based on your interests, run and optimize marketing campaigns, measure the performance of ads and content, and derive insights about the audiences who engage with ads and content. This data is an integral part of how we operate our site, make revenue to support our staff, and generate relevant content for our audience. You can learn more about our data collection and use practices in our Privacy Policy.

If you wish to request that your personal information is not shared with third parties, please click on the below checkbox and confirm your selection. Please note that after your opt out request is processed, we may still collect your information in order to operate our site.



I want to make a 'Do Not Sell My Personal Information' request. Note: this action will make it harder to us to tailor content for you.

CONFIRM

[Data Deletion](#)

[Data Access](#)

[Privacy Policy](#)

Example 2: Forever 21 (<https://www.forever21.com/us/shop/info/optout>), visited 10/27/20

Please note the language in this notice that attempts to minimize the effects of cookie tracking (“data contained in these Cookies does not typically identify you,” warns the consumer that avoiding tailored ads “may not be what you want,” and informs consumers that even after they exercise their rights, “we will still continue to share data with our service providers.” Finally, the company uses this notice to argue with the definition of the term “sale” in the CCPA, attempting to delegitimize the regulation.



Do Not Sell My Info

The CCPA gives California consumers the right to opt-out of the sale of their personal information (“PI”).

The only way you can exercise this right as it relates to the use of cookies and other tracking technologies, is to click on the Do Not Sell My Information Toggle below from each browser and device you use.

However, before you click on the Do Not Sell My Information Toggle below, we hope that you will consider a few more things:

- First, remember that the data contained in these Cookies does not typically identify you by name or other directly identifiable means.
- Second, opting-out of sales of your PI in the digital advertising context (i.e. by means of Cookies) will not stop you from getting ads, but these ads will not be tailored to your interests. This may not be what you want.
- Third, if you opt-out, your experience on our Sites and when you otherwise engage with us will be much less personalized.
- Fourth, even after you opt-out, we will still continue to share data with our service providers who use the data on our behalf.

The CCPA defines “sale” in an unusual way, and with no guidance yet from the State of California as to how broadly the term should be interpreted, a number of differing reasonable interpretations are possible.

Some may argue that when certain third parties place Cookies on the consumer’s device when the consumer engages with our site or app, the PI collected by such Cookies constitutes a “sale” under the CCPA. We do not agree with this interpretation. However, pending a consensus as to what “sale” actually means under the CCPA, we are providing a way for California consumers to opt-out of future Cookie-based “sales” of their PI, by (i) enabling the Google Restricted Processing solution into our use of certain Google products, (ii) using the IAB Tech Lab “do not sell” signal with third parties that we work with and that are participating in the IAB CCPA Compliance Framework, and (iii) disabling other third parties’ Cookies that are not covered by either (i) or (ii) above. The solutions referenced in (i) and (ii) each conveys to the recipient that PI can only be used for restricted purposes, such as providing us services, and cannot be sold by the recipient downstream. We make no guaranty as to how third parties will treat our Do Not Sell signals.

Appendix 5: Example of opt-out form nested beneath excessive text Home Depot (<https://www.homedepot.com/privacy/Exercise My Rights>), visited 10/27/20 Please note: this screenshot includes only the top portion of the webpage

Home / Exercise Privacy Rights

The Home Depot & Your Personal Information

MOST VIEWED

- Check Order Status
- Store Finder and Store Hours
- My Account Sign In
- Check Order History
- Order Cancellation
- Shipping and Delivery FAQ
- Pay Credit Card Bill
- About My Order**
- Check Order Status
- Order Cancellation
- Confirm Order Was Placed
- Shipping and Delivery FAQ
- In-Store Pickup
- Shipping and Delivery**
- Free Shipping
- Shipping Options
- Buy Online and Pickup in Store
- Buy Online and Ship to Store
- Check Order Status
- Shipping and Delivery FAQs
- Product and Services**
- Product Availability
- Protection Plans
- Installation Services
- Tools and Truck Rental
- Moving Services
- Pro Services
- How To and Project Guides
- Ratings and Reviews
- Seeds Program
- Pricing and Promos**
- Price Match Policy
- Savings Center
- LocalAd
- Special Buy of the Day
- Credit Center
- Credit Offers
- Rebate Center
- Payments**
- Payment Methods
- Gift Cards and Store Credits
- Tax Exemptions
- Credit Card Bill Payments
- My Account**
- Order History
- In-Store eReceipts
- Email/phone Opt-in/out
- Credit Card Payments
- Returns and Recalls**
- Online Purchase Return Policy
- In-Store Purchase Return Policy
- Recalls
- Policies and Legal**
- Terms of Use
- Exercise My Privacy Rights
- Privacy and Security Statement
- Manage My Marketing Preferences
- California Rights and Regulations
- Electronics Recycling Programs
- The Home Depot Reviewer Program
- Corporate Information**
- Careers
- Corporate Information
- Home Depot Foundation
- Government Customers
- Investor Relations
- Suppliers and Providers

The Home Depot values and respects your privacy. Some of the ways we use the information we collect include:



CONVENIENCE

To provide you with the best shopping experience through services like eReceipts, home delivery, and in-store pickup.



CONSISTENCY

To provide the same customer service experience when you engage with us in our stores, online, or over the phone.



COMMUNICATION

To provide the same customer service experience when you engage with us in our stores, online, or over the phone.



AWARENESS

To make you aware of the products and services we offer to support your home improvement needs.

You can learn more about how The Home Depot uses the personal information we collect in our [Privacy and Security Statement](#).

Exercise Your Privacy Rights

Complete the form below to submit your request. When we receive your information, we'll use it to verify your identity and review your request. You can only submit one type of request at a time. Need to make more than one request? Complete a new submission form for each request.

You can:

- Request the personal information we collect about you.
- Ask that we delete the personal information we collect about you.
- Submit an Opt Out of Sale request (while we do not share your personal information with third parties in exchange for money, we disclose certain information in exchange for insights and other valuable services, and California law treats such sharing as a "sale" even if no money is exchanged; click here for more information).

IMPORTANT NOTE REGARDING REQUESTS TO OPT OUT OF SALES

When you visit our website, we use cookies and similar tools to automatically make certain personal information available to select third parties who are providing services to us to help us enhance your experience, improve and deliver advertising, learn how you use the website, and achieve the other purposes addressed in the "Tracking Tools We Use" section of our [Privacy and Security Statement](#). Some of those select third parties may use the personal information for their own purposes or to provide services to other businesses. California law treats such sharing as a "sale" even if no money is exchanged.

If you want to opt out of such automatic sharing, use this form to submit an Opt Out of Sale request, and we will place a cookie on your browser to automatically prevent the sharing from happening when you use that browser to visit our website. Because we use a cookie to automatically identify and register your preference, if you disable cookies on your browser or device, the Opt Out of Sale request will no longer work. You can always enable cookies on your browser or device and visit this page again to register your Opt Out of Sale request. We may not recognize you when you use other browsers or devices to visit our website. So, you will need to submit a separate Opt Out of Sale request on each device and browser you use to visit our website. For more information about our tracking tools and how to control them, please click here.

After you submit an Opt Out of Sale request, you may still see advertising regarding our products and services. And some of that advertising may be delivered by third parties or appear on third-party sites or services. This advertising may be general audience advertising or may be delivered by service providers in ways that do not involve sales of your personal information.

When you submit your Opt Out of Sale request using the form below, as indicated above, we will no longer share your information via digital tracking technologies used on homedepot.com. You may need to take other steps for other websites, as described in the privacy policies for those websites. We also will use the information you provide via the form to identify the personal information not involving online tracking technologies that we hold about you so that we can honor your request that such information no longer be sold as well.

Once you submit your request, we will place a cookie on your browser to automatically prevent the sharing from happening when you use the browser to visit our website. However, to fully register your Opt Out of Sale request for information that may be shared via channels other than online tracking technologies, if any, you will need to provide a working email address and respond to the verification request we send you.

Making a Request

A working email address is required to complete your request online. Call 1-800-394-1326 to speak to a representative if you don't want to provide an email address.

For each request you submit, we'll send a verification email to the email address you provided. This may take up to 72 hours. Check your spam folder if you don't see it. You'll have 3 days to verify your email before your request expires. If you don't, you'll have to submit another request.

If you are making a request on behalf of another person, please send your request to myinfo@homedepot.com and include the following information about you and the person on whose behalf you are making the request: full name, mailing address, email address, and phone number. You should also provide proof of your authorization to act on the other person's behalf. We will contact you for additional information once your request has been received.

After we process your request to delete your personal information or to Opt Out of Sale, you may still see advertising regarding our products and services. We may deliver advertising to a general audience or place advertising on websites, mobile applications, and connected device applications that relates to our products and services. For example, if you visit a do-it-yourself website, you may see advertising on that website that promotes our products and services related to the do-it-yourself content.

Submit Your Privacy Request

Select Request Type

- Get My Information Delete My Information Opt Out of Sale

First Name

Last Name

State of Residence

Email Address

W392-1
cont

Appendix 6: Examples of instructions for opt-outs based on cookie tracking

Please note: the BuzzFeed, Los Angeles Times, Verizon Media, and Warner Media examples used in the earlier appendices are also examples of the confusing and multi-step processes consumers must follow to ensure that their DNS requests are respected by companies relying on third party tracking mechanisms. In the examples below, consumers are instructed that they will have to replicate the process for making their requests using every browser on every device they have used to access these websites.

Example 1: Office Depot cookie example (visited 10/22/20)

IMPORTANT NOTE REGARDING REQUESTS TO OPT OUT OF SALES

When you visit our website, we use cookies and similar tools to automatically make certain personal information available to select third parties who are providing services to us to help us enhance your experience, improve and deliver advertising, learn how you use the website, and achieve the other purposes addressed in the "Tracking Tools We Use" section of our [Privacy and Security Statement](#). Some of those select third parties may use the personal information for their own purposes or to provide services to other businesses. California law treats such sharing as a "sale" even if no money is exchanged.

If you want to opt out of such automatic sharing, use this form to submit an Opt Out of Sale request, and we will place a cookie on your browser to automatically prevent the sharing from happening when you use that browser to visit our website. Because we use a cookie to automatically identify and register your preference, if you disable cookies on your browser or device, the Opt Out of Sale request will no longer work. You can always enable cookies on your browser or device and visit this page again to register your Opt Out of Sale request. We may not recognize you when you use other browsers or devices to visit our website. So, you will need to submit a separate Opt Out of Sale request on each device and browser you use to visit our website. For more information about our tracking tools and how to control them, please [click here](#).

Example 2: Walmart cookie example (visited 10/22/20)

We respect the privacy of your personal information. The information you provide here will only be used to process your opt out of sale request. To assure the implementation of your request across all devices associated with your account, you should login to your account with each of your devices. If you are not logged in or do not provide accurate account details, you should complete an opt out of sale request on each browser or device that you use to access our websites and mobile services. In addition, if you are not logged into your account while making your request, and you later clear your Walmart cookies, your opt out of sale request will need to be resubmitted. Please note that your request will apply to future sales of your personal information and will not impact sales made prior to your request.

From: [Rachel Nemeth](#)
To: [Privacy Regulations](#)
Subject: CTA Letter on Third Set of Proposed Modifications to Proposed CCPA Regulations
Date: Wednesday, October 28, 2020 4:33:28 PM
Attachments: [CTA Letter on Third Set of Modifications to Proposed CCPA Regulations-FINAL.pdf](#)

See attached for comment letter from Consumer Technology Association (CTA).

Thank you,
Rachel

Rachel Sanford Nemeth

Sr. Director, Regulatory Affairs
Consumer Technology Association, producer of CES®

[REDACTED]

d: [REDACTED]

c: [REDACTED]

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).

October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Dear Ms. Kim:

Consumer Technology Association (“CTA”)¹ respectfully submits this letter commenting on the third set of modifications to the proposed California Consumer Privacy Act (“CCPA”)² regulations.³ As CTA has previously explained, since the CCPA was signed into law, companies of all sizes have raced to establish processes, policies, and systems to come into compliance. For many, this effort has already been a significant, challenging and expensive initiative.⁴

CTA therefore supported those changes in the initial and second set of modifications that sought to reduce some of the confusion regarding businesses’ regulatory requirements. CTA now recommends changing Proposed Section 999.306—Notice of Right to Opt-Out of Sale of Personal Information—to provide more clarity and predictability for the many businesses that have implemented CCPA requirements in good faith and to avoid consumer confusion.

The Department should clarify that the new offline notice requirement applies when only a business both collects and *sells* data from offline activity. Many businesses do not sell data collected during offline activities such as store visits. For businesses that do not sell data

W393-1

¹ As North America’s largest technology trade association, CTA^o is the tech sector. Our members are the world’s leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES^o—the most influential tech event on the planet.

² Cal Civ. Code § 1798.100 *et. seq.*

³ See California Department of Justice, Notice of Third Set of Modifications to Text of Proposed Regulations, OAL File No. 2019-1001-05 (Oct. 12, 2020).

⁴ See Comments of Consumer Technology Association on Proposed Adoption of California Consumer Privacy Act Regulations (filed Dec. 6, 2019); Comments of Consumer Technology Association on Modifications to Proposed Regulations (filed Feb. 25, 2020); Comments of Consumer Technology Association on Second Set of Modifications to Proposed Regulations (filed Mar. 27, 2020).

Producer of



collected during such offline activities, but sell data collected online, an offline notice will create consumer confusion by falsely implying to consumers that it does. Even if such a notice does not directly cause consumer confusion, an additional offline notice would be redundant and burdensome to businesses that must already provide two forms of opt-out notice.⁵

CTA agrees that a company should offer an offline notice when data that is collected offline may be sold. Accordingly, the Department should make the following targeted edits to Proposed Section 999.306(b)(3):

- (3) A business that collects personal information in the course of interacting with consumers offline **and sells such information** shall also provide notice by an offline method that facilitates consumers' awareness of their right to opt-out. Illustrative examples follow:
- a. A business that collects personal information from consumers in a brick-and-mortar store **and sells such information** may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.
 - b. A business that collects personal information over the phone **and sells such information** may provide the notice orally during the call where the information is collected.

W393-1
cont

CTA appreciates the Department's continued efforts to adopt and implement CCPA regulations in a manner that enhances consumer privacy without being unduly burdensome on businesses, especially startups and other small businesses. With the recent adoption of final regulations in August, CTA encourages the Department to condition any modification to CCPA regulations on providing additional clarity to both businesses and consumers, reducing still-remaining unjustified burdens on businesses, and ensuring that the regulations properly adhere to the requirements of the statute. The above suggested modifications will help accomplish these goals.

Respectfully submitted,

/s/ Michael Petricone
Michael Petricone
Sr. VP, Government and Regulatory Affairs

/s/ Rachel Nemeth
Rachel Nemeth
Senior Director, Regulatory Affairs

⁵ Cal Civ. Code § 1798.135(1)-(2); Cal. Code Regs. Tit. 11 § 999.306(b)(1)-(2).

From: [Javier A. Bastidas](#)
To: [Privacy Regulations](#)
Cc: [Lara L. DeCaro](#)
Subject: Comments to Proposed Modified CCPA Regulations [OAL File No. 2019-1001-05]
Date: Wednesday, October 28, 2020 4:44:16 PM
Attachments: [Comments to Third Set of Proposed Modified CCPA Regulations \(01629220x9C6B5\).pdf](#)

Dear Deputy Attorney Kim:

Attached please find our law firm's comments to the Third Set of Proposed Modifications to the CCPA Regulations.

If you have any questions regarding these comments, please do not hesitate to contact us.

Thank you for your time,

Javier Bastidas

Javier A. Bastidas

Leland, Parachini, Steinberg, Matzger & Melnick LLP

199 Fremont Street, 21st Floor

San Francisco, CA 94105

Telephone: 415.957.1800

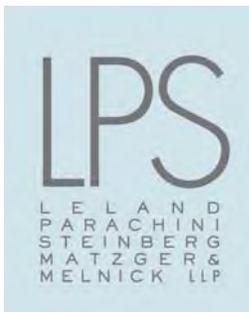
Direct: [REDACTED]

Mobile: [REDACTED]

Think Green! Before printing this e-mail ask the question, is it necessary?

CONFIDENTIALITY:

The e-mail is intended solely for the use of the individual to whom it is addressed and may contain information that is privileged, confidential or otherwise exempt from disclosure under applicable law. If the reader of this e-mail is not the intended recipient or the employee or agent of the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by replying to the original sender of this note or by telephone at 415.957.1800 and delete all copies of this e-mail. It is the recipient's responsibility to scan this e-mail and any attachments for viruses. Thank you.



LARA L. DECARO
[REDACTED]
JAVIER A. BASTIDAS
[REDACTED]

October 28, 2020

Sent via electronic mail

Deputy Attorney General Lisa B. Kim,
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Re: **Comments to the Third Set of Proposed Modified Regulations Concerning the California Consumer Privacy Act ("CCPA")**

Dear Deputy Attorney General Kim:

On behalf of our law firm, Leland, Parachini, Steinberg, Matzger & Melnick, LLP, we respectfully provide the following comments concerning the Third Set of Proposed Modified Regulations for the CCPA (the "Regulations"). We appreciate and applaud the Attorney General's efforts to clarify and improve upon the previous, existing regulations. In this comment round, we focus on only the most important matters to our clients as we recognize the grand task ahead of you.

A. ENABLING LEGISLATION.

The Attorney General derives its authority for the proposed Regulations, in part, from California Civil Code Section 1798.185(a), which reads:

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

[...]

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

{999/0001/LTR/01629186.DOCX}

199 FREMONT STREET, 21ST FLOOR ■ SAN FRANCISCO, CA 94105
PHONE 415.957.1800 ■ FAX 415.974.1520 ■ WWW.LPSLAW.COM

CCPA_3RD15DAY_00152



(4) Establishing rules and procedures for the following:

[...] (C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

[...]

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

B. ANALYSIS OF PROPOSED REGULATIONS.

I. EXCEPTIONS FOR TRADE SECRETS AND INTELLECTUAL PROPERTY RIGHTS

Thus far, there are no provisions concerning the exceptions mandated by Section 1798.185(a)(3) though previous commentators have noted the deficiency. The Attorney General argued that “the comments fail to show how an exemption for protection of intellectual property rights is necessary” as they “fail to explain how a consumer’s personal information collected by the business could be subject to the business’s copyright, trademark, or patent rights, or how a business could possibly patent, trademark or copyright a consumer’s personal information” (Response 901/Appendix A). The Attorney General’s responses also noted that even if a consumer’s personal information could potentially be considered a trade secret, “neither federal nor state law provides absolute protection for trade secrets” (*Id.* at Response 247/). The Attorney General further concluded that “a blanket exemption from disclosure for any information a business deems could be a trade secret or another form of intellectual property would be overbroad and defeat the Legislature’s purpose of providing consumers with the right to know information businesses collect from them” (*Id.*)

W394-1

Respectfully, Section 1798.185(a)(3) states nothing about "blanket" exemptions nor are businesses seeking "absolute" protection. It is also not the duty of the public to delineate the specific exceptions contemplated by the above statute. The legislators tasked the Attorney General's office to adopt the appropriate language, after receiving comment from the public. While there is no doubt that the legislature intended to provide consumers with the right to know about the information that businesses collect, it was also the legislature's clear intent to provide some



exceptions in this context, including but not limited to those concerning trade secrets and other intellectual property rights.

For example, we point to the obligation within the Notice of Financial Incentive portion of the Regulations (Section 999.307(b)(5)¹), requiring businesses to provide a “good-faith estimate of the value of the consumer’s data.” Such disclosure as required by the Regulation may involve proprietary information, which Section 3426.1 of California’s Uniform Trade defines as follows:

(d) “Trade secret” means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
- (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

W394-1
cont

It is reasonable to conclude that companies may wish to keep their proprietary methods for such a calculation a secret. While we agree that a consumer has a right to know what information is collected, where is the authority requiring a company to disclose its formulas for calculating the economic value contemplated by Regulation 999.307(b)(5)? It simply does not exist.

Therefore, the easy fix is to delete Section 999.307(b)(5) from the Regulations and to compose new regulations that address the legislature's concerns over trade secrets, intellectual property rights, and other possible exceptions needed to comply with other State and Federal laws. Once the Attorney General has drafted such new language, then the public can provide meaningful comments regarding the new language in a future comment period.

II. DEVELOPMENT OF OPT-OUT LOGO OR BUTTON

Again, the Attorney General has failed to develop a "recognizable and uniform opt-out logo or button" as required by Section 1798.185(a)(4)(C) of the Civil Code (see above). While the original proposed regulations had provided for an Opt-Out switch, those provisions were

W394-2

¹ (b) A business shall include the following in its notice of financial incentive... (5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including: a. A good-faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference; and b. A description of the method the business used to calculate the value of the consumer’s data.



deleted from subsequent iterations of the Regulations. Such a logo or button would greatly simplify the Opt-out process and bring clarity to businesses throughout the state and beyond.

Newly proposed Regulation 999.315(h) provides the following:

(h) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out...

(1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.

(2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to optout.

While we appreciate the Attorney General's attempts to clarify the opt-out rules, we believe that the confusion that exists in this regard can be avoided by propounding the adoption of a uniform opt-out button. We agree the Notice language should be simple to understand, and we support the notion behind subsection (h)(2), but creating a recognizable device for the public to use will eliminate the confusion companies are currently experiencing in figuring out what language is legally sufficient for their requisite Notices. While the new Regulation language provides some helpful guidance, it is still too complicated. There will be no need for measuring the "number of steps" towards opt-out versus opt-in procedures when a recognizable button can accomplish what the legislature intended in just one-step.

W394-2
cont

III. ACCESSIBILITY

While our firm of course supports the requirement that all website notices be "reasonably accessible to consumers with disabilities," respectfully, we believe that the Attorney General's office has overstepped its authority by introducing language, in essence new law, concerning the use of "Web Content Accessibility Guidelines" or "WCAG." The United States Department of Justice ("DOJ") has urged that "public accommodations have flexibility in how to comply with the ADA's general requirements of nondiscrimination and effective communication" (see letter dated September 25, 2018, from Assistant General Stephen E. Boyd²). Furthermore, in *Robles v.*

W394-3

² <https://www.adatitleiii.com/wp-content/uploads/sites/121/2018/10/DOJ-letter-to-congress.pdf>



Domino's Pizza, LLC (2019) 913 F.3d 898, the Ninth Circuit held that the ADA was intended to give businesses "maximum flexibility" in meeting the statute's requirements.

"A desire to maintain this flexibility might explain why DOJ withdrew its [Advanced Notice of Proposed Rulemaking] related to website accessibility and 'continue[s] to assess *whether specific technical standards are necessary and appropriate* to assist covered entities with complying with the ADA.'" (*Id.* at 908-909, citing 82 Fed. Reg. 60921-01 (December 26, 2017) [emphasis in original]).

Furthermore California Civil Code Section 1798.185(a)(6) states that the Attorney General shall establish rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer. It follows that businesses can provide the requisite notices in a manner that is easily understood if the regulations dictating the requirements were also easily understood.

Here we are in late October 2020, and the Regulations have still not been finalized in reality. How can a company truly be held to all CCPA requirements under such circumstances? Add to that, the fact that, as a result of the on-going Covid-19 pandemic, businesses have been forced to furlough or fire employees who have relevant knowledge and responsibility for CCPA compliance. Businesses have also been forced to reduce their outside counsel due to pandemic-related budget shortfalls.

In this environment, aside from the legislative overstep on the part of the Attorney General, it simply does not make any sense to introduce the new WCAG requirements when such rules complicate the question of what the Regulations require, and create new, substantial costs for all on-line companies. Further, there's no evidence that these WCAG requirements are truly "generally recognized industry standards" for on-line information accessibility. In fact, both the DOJ and the Ninth Circuit hold positions that contradict this proposition.

In the Attorney General's own words (See "Final" Statement of Reasons published on June 1, 2020):

"DOCUMENT INCORPORATED BY REFERENCE The following document is incorporated in the regulations by reference: World Wide Web Consortium, Web Content Accessibility Guidelines (WCAG) 2.1 (June 5, 2018) [as of May 21, 2020]. The document is incorporated by reference because it would be *cumbersome, unduly expensive, or otherwise impractical* to publish the document in the California Code of Regulations..." (emphasis added).

In other words, the Attorney General appears to expect companies to follow the voluminous and admittedly "cumbersome" WCAG requirements, even though the CCPA makes no mention of it

W394-3
cont



and the DOJ strongly advise flexibility in compliance. In short, the WCAG rules, aside from being unconstitutional (as fully explained in our previous comment dated and submitted on February 25, 2020), creates a scenario that makes it practically impossible for companies to successfully achieve CCPA compliance because companies cannot provide "simple" notices when the rules behind them are so terribly complex.

W394-3
cont

Thank you for your time and consideration of these comments.

Very truly yours,

A handwritten signature in blue ink that reads "LDe /s/".

Lara L. DeCaro
LELAND, PARACHINI, STEINBERG,
MATZGER & MELNICK, LLP

A handwritten signature in blue ink that reads "JAB /s/".

Javier A. Bastidas
LELAND, PARACHINI, STEINBERG,
MATZGER & MELNICK, LLP

From: [Halpert, Jim](#)
To: [Privacy Regulations](#)
Subject: State Coalition -- Final Comments re AG_s Office CCPA Do Not Sell Notice Rules October 28, 2020.DOCX
Date: Wednesday, October 28, 2020 5:01:08 PM
Attachments: [State Coalition -- Final Comments re AG_s Office CCPA Do Not Sell Notice Rules October 28, 2020.DOCX](#)

Enclosed are our comments on the latest proposed rules changes.

Thank you for your consideration – Jim Halpert

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

State Privacy and Security Coalition, Inc.

October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Department of Justice
300 Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Comments Regarding Title 11(1)(20): Third Set of Proposed Modification of Text of Regulations

I. Introduction

The State Privacy & Security Coalition is a coalition of 29 companies and 7 trade associations across the retail, payments, communications, technology, fraud prevention, tax preparation, automotive and health sectors. We work for laws and regulations at the state level that provide strong protection for consumer privacy and cybersecurity in a consistent and workable matter that reduces consumer confusion and unnecessary compliance burdens and costs.

Our Coalition worked with Californians for Consumer Privacy and consumer privacy groups on amendments to clarify confusing language in the CCPA, to reduce the risk of fraudulent consumer requests that would create risks to the security of consumer data, and to focus CCPA requirements on consumer data, consistent with the title of the law.

We agree with the with the proposed additions laid out in § 999.315(h) regarding not creating barriers to the choice to opt out, and suggest one clarification highlighted below. However, we are concerned about the changes proposed in 999.306(b) because of the risk of consumer confusion and therefore oppose these modifications. Only when a business actually sells personal information collected through the offline channel should a notice of the right to opt out be required.

We further oppose the change to § 999.326(a), which would in the case of right to know and data deletion requests bar businesses from both asking the consumer to verify their identity and to confirm that the authorization presented by the authorized agent is actually from the consumer.

1. We agree with that businesses should not interfere with user opt-out requests.

Our Coalition agrees that businesses should not create barriers to consumers executing opt-out requests for actual sales of personal data. We suggest only a minor clarification with regard to the proposed restrictions in § 999.315(h)(3) -- that the business may explain truthfully the effect of an opt-out request (as the First Amendment to the U.S. Constitution would require).

W395-1

State Privacy and Security Coalition, Inc.

- 2. We urge clarifying that the additions to the notice of the right to opt-out in § 999.306(b)(3) apply only if the information collected through the applicable offline channel (i.e., in a brick or mortar store or over the phone) is in fact sold.**

Providing a notice of the right to opt-out in offline channels should be required only in situations where personal information collected through the offline channel is sold. To do otherwise would, for example, lengthen telephone interactions with consumers and could require notices in stores when the personal information collected through that channel is never sold. This would be confusing and misleading to consumers, as it would be suggesting to them that the information being collected in that channel is in fact to be sold, when in fact it is not.

Furthermore, if the consumer made a “do not sell” request through the offline channel, the business would in most situations be unable to relate that request to the other channel through which personal information collected is being sold without collecting significantly more personal information – a step that Civil Code § 1798.145(k) of the CCPA specifically makes clear that the statute does not require. The end result would be even more confusing and frustrating for consumers.

W395-2

On the other hand, if personal data collected by a business through the offline channel is sold, then an opt-out notice should be required. In addition, because notice may be provided “at or before the time of collection”, in the brick and mortar store context, we suggest that “at the store entrance” be included as one of the illustrative examples set forth in § 999.306(b)(3)a.

W395-3

In the brick and mortar store context, personal information can sometimes be collected outside the store anywhere in the parking lot. For this reason, we suggest an illustrative example for collection of personal information outside the store.

Finally, we suggest that, like subdivision 3a (in-store notice), subdivision 3b (telephone notice) similarly refer to the option of directing consumers to where the notice can be found online. This clarification would be consistent with both subdivision 3a. and with § 999.305(b)(3).

W395-4

For all these reasons, we ask that the final regulations insert the phrase “that it sells” in subdivision (3), as well as clarify subdivisions (3)a. and b. as follows:

(3) A business that collects personal information in the course of interacting with consumers offline that it sells shall also provide notice by an offline method that facilitates consumers’ awareness of their right to opt-out. Illustrative examples follow:

- a. A business that collects personal information from consumers in a brick-and-mortar store may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage directing consumers to where the notice can be found online by the store entrance, ~~or~~ in the area where the personal information is collected, or, if personal information is collected outside the store, in an area that is reasonably visible to consumers directing consumers to where the notice can be found online.**

W395-2
W395-3
and
W395-4

State Privacy and Security Coalition, Inc.

b. A business that collects personal information over the phone during the call where the information is collected may provide the notice aurally or aurally direct consumers to where the notice can be found online ~~aurally during the call where the information is collected.~~

W395-2
W395-3
W395-4
cont

These language additions would clarify when and what sort of notice is in fact required and would alleviate consumer confusion.

3. **The proposed restriction in § 999.326(a) on authenticating third party right to know and data deletion requests should be clarified or stricken in the final rule to reduce risk of pretexting and fraud.**

The Final Rules rightly impose greater authentication requirements for right to know and data deletion requests because of the security and privacy risks these rights pose if wielded by fraudsters or hackers. The very same reasons counsel strongly against cutting back on business' leeway to authenticate right to know and data deletion requests filed by a purported authorized agent.

We are unclear about the rationale for shifting the submission of proof of the signed permission authorizing the agent from the consumer to the authorized agent. While the addition of such an option might be workable, allowing a business to do only one (and not both) of further authentication steps risks increased fraud.

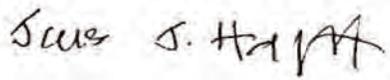
W395-5

We request the following amendment to § 999.326(a), as follows:

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do ~~either of do~~ the following:

A business should be allowed both to require the consumer to verify their identity with the business *and* to confirm with the business that they provided the authorized agent permission to submit the request. Both are *very important* to prevent fraudulent requests to delete or obtain the contents of a consumer account when a pretexter has established a fake account in the same name as the consumer, thereby making the fake account appear more real.

Respectfully submitted,



Jim Halpert, Counsel
State Privacy & Security Coalition

From: [Aleecia M McDonald](#)
To: [Privacy Regulations](#)
Cc: [Mingya Feng](#); [Zeeshan Sadiq Khan](#); [Bingxuan Luo](#); [Xiaofei Ma](#); [Arjita Mahajan](#)
Subject: Re: NOTICE OF THIRD SET OF PROPOSED MODIFICATIONS TO TEXT OF CCPA REGULATIONS
Date: Wednesday, October 28, 2020 5:01:40 PM
Attachments: [McDonaldEtAl-Comments-to-AG-CCPA-Oct28-Rulemaking.pdf](#)

Thank you for the opportunity to provide comments, as enclosed.

Aleecia

Assistant Professor Aleecia M. McDonald // Carnegie Mellon's Information Networking Institute //



Comments from:

Maggie Feng [REDACTED], Zeeshan Sadiq Khan [REDACTED],
Bingxuan Luo [REDACTED], Xiaofei Ma [REDACTED],
Information Networking Institute
Carnegie Mellon University
4616 Henry Street
Pittsburgh, PA 15213

Arjita Mahajan [REDACTED],
Professor Aleecia M. McDonald (corresponding author) [REDACTED]
NASA Ames Research Center
Carnegie Mellon University
Building 23
Moffett Field, CA 94035

October 28, 2020

Lisa B. Kim
Privacy Regulations Coordinator California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Regarding

Sections 999.300 through 999.341
of Title 11, Division 1, Chapter 20,
of the California Code of Regulations (CCR)
concerning the California Consumer Privacy Act (CCPA)

About the Authors

Maggie Feng is a graduate student at Carnegie Mellon University pursuing her Master's in Information Security. She is currently part of the CCPA browser tool team under Professor McDonald's supervision, worked on the front end, and designed the authentication system.

Zeeshan Sadiq Khan is a graduate student at Carnegie Mellon University pursuing his Master's in Information Security. Inspired by the Do Not Track specification, he has designed a similar specification to signal to the web servers Californian's data privacy preferences for CCPA use.

Bingxuan Luo is a graduate student at Carnegie Mellon University pursuing a Master's degree in Information Technology Mobility. She was a previous intern at Facebook. On the CCPA browser tool, she designed the UI and user interaction flow, and helped integrate the API with the back end.

Xiaofei Ma is a graduate student at Carnegie Mellon University pursuing her Master's in Information Technology. She designed features to send Californian's data privacy preferences to both first-party and third-party companies in the CCPA browser tool.

Arjita Mahajan is a graduate student at Carnegie Mellon University pursuing her Master's in Software Management. She has 5 years of work experience in Software Engineering and has worked on GDPR requirements professionally. She works as Program Manager for the browser tools team and helps engineering team coordination and requirements planning with Professor McDonald.

Aleecia M. McDonald is an Assistant Professor at Carnegie Mellon's Information Networking Institute, based in Silicon Valley. Her *Psst!* Lab focuses on researching the public policy issues of Internet privacy including user expectations, behavioral economics and mental models of privacy, and the efficacy of industry self-regulation. She co-chaired the WC3's Tracking Protection Working Group, a multi-national effort to establish international standards for a Do Not Track mechanism that users can enable to request enhanced privacy online. She presented testimony to the California Assembly including regarding the California Consumer Privacy Act, contributed to testimony before the United States Senate, and presented research results to the Federal Trade Commission. Professor McDonald is a member of the Board of Directors for the Privacy Rights Clearinghouse, and is a member of Carnegie Mellon's CyLab. She was Director of Privacy at the Stanford Center for Internet and Society where she maintains a non-resident Fellow affiliation. She was also previously a Senior Privacy Researcher for Mozilla during the rollout of Do Not Track in the Firefox web browser. A decade of experience working in software startups adds a practical focus to her academic work. She holds a PhD in Engineering & Public Policy from Carnegie Mellon.

Affiliations are for identification and context only. These comments reflect the authors' views alone; we do not speak for any other groups, including Carnegie Mellon University.

Summary

In this comment we urge the following three courses of action:

1. Adding a new subsection, § 999.315 (h) (6) Opt-out preferences must persist for at least as long as opt-in preferences.
2. Adding a new function for the AG's office to facilitate centralized opt-out for data that is indexed by non-technical PII including name, address, and phone number akin to the FTC's Do Not Call list. The AG's office would therefore become an Authorized Agent under revised § 999.326.
3. Similar to the AG's prior work on *Privacy on the Go: Recommendations for the Mobile Ecosystem* <https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf> we call on the AG's office to convene dialogs regarding the technical mechanisms for CCPA rights. We see some current offerings do not yet fulfill legal requirements for children's opt-out consent in § 999.332.

Table of Contents

Background: Building Tools to Enacting Privacy Choices	4
Topic 1: Changes to § 999.315 Requests to Opt-Out	4
Topic 2: Creating a Do Not Sell Database within the California AG’s Office	4
Recommendation:	6
Topic 3: Tools for CCPA Compliance	6
Recommendation:	9

Background: Building Tools to Enacting Privacy Choices

Thank you for the opportunity to comment on the proposed rulemaking around the California Consumer Privacy Act (CCPA.) As part of our Practicum course at Carnegie Mellon, this semester a team of five students is currently prototyping *Data Guard*. The Data Guard project is a collection of technical tools and user education to support CCPA rights in an automated way, in order to reduce the user burden of asserting CCPA rights.

During our work on Data Guard we encountered areas we see a role for the California Attorney General’s (AG’s) office to host data that would support realizing Californian’s data privacy rights. In particular, we recommend a structure parallel to the FTC’s hosting of Do Not Call phone numbers *in addition* to other technical measures that are under development. Second, we also note parallel similar efforts from multiple groups, and hope the AG’s office will take a formal interest in tools that meet business’ legal requirements under add legal section here.

Topic 1: Changes to § 999.315 Requests to Opt-Out

We support the proposed addition of (h) to § 999.315, which contains common-sense requirements to avoid “dark patterns” on the web that discourage user choice. In addition, we propose: | W396-1

§ 999.315 (h) (6) Opt-out preferences must persist for at least as long as opt-in preferences. For example, if a user is able to opt-in indefinitely without further contact, then a company must not present daily opt-out dialogs. | W396-2

Topic 2: Creating a Do Not Sell Database within the California AG’s Office

Under the CCPA, businesses are required to provide a “Do Not Sell My Info” link on their sites. With visible links, consumers can exercise their privacy rights from first parties, but they are often not aware of the data collection from third parties. Indeed, one of the major advantages to an automated header request is that it reaches all parties, including invisible third parties. However, this is of limited use for historic third-party data collection with data still in use. | W396-3

Data brokers can still collect consumers’ data without any direct interaction. In this case, consumers may not be informed that their data is collected by unknown parties. How to practice their CCPA rights can be unclear.

To solve this problem, CCPA requires all data brokers to register with AG's office and provide information about how to opt out for consumers. Although the data broker listing is accessible to consumers, it's extraordinarily difficult for consumers to follow the instructions and manually opt-out 407 companies.¹

Californians might like to automatically notify data brokers of one of two things:

1. The user is a child (and therefore must be asked to consent to opt-in to data use)
Or
2. The user is an adult, and hereby opts of data use

There is a technical obstacle to realizing CCPA rights. One might imagine simply sending an HTTP header signal to all data brokers once a year to advise them of childhood or opt-out, but such a system of broadcasting HTTP headers fails to work. Third parties, such as data brokers, can (typically) only read their own cookies when a user happens to visit a first-party website at the same time the third-party website is also part of the communication. With 407 data brokers, it could take quite a while to bump into all of them. During that time, children's data and the data from those who try to opt-out would still be bought, sold, and used.

Large companies run into this issue too. They might have multiple domains (e.g. google.com and youtube.com are both part of the same corporate structure, but have different technical structures.) Major companies such as Warner Media (including cnn.com),² Walmart³, and Oracle⁴ use email as an identifier to assist users with the opt-out process, not just within their own company, but as an identifier they send to third party partners. Other potential (mostly) unique identifiers include telephone number, address, and/or name.

In order to help consumers exercising their CCPA rights with data brokers, we designed a feature in our Data Guard CCPA browser tool. Users of our tool can send requests to all data brokers, identifying the user by email address. A screenshot of the tool can be seen in Figure 1.

W396-3
cont

¹ "Data Broker Registry." State of California - Department of Justice - Office of the Attorney General, 22 Oct. 2020, oag.ca.gov/data-brokers. Accessed 28 October 2020.

² "CNN opt-out form." WarnerMedia Privacy Center, www.warnermediaprivacy.com/do-not-sell/request/. Accessed 28 October 2020.

³ "Walmart opt-out inquiry form." Walmart, cpa-ui.walmart.com/affirmation. Accessed 28 October 2020.

⁴ "Oracle opt-out inquiry form." Oracle, www.oracle.com/legal/data-privacy-inquiry-form.html. Accessed 28 October 2020.

Data Broker

"Data broker" means a business that doesn't have direct relationship with you but collect your information. Imagine a website you never visit before collecting your information and exchange for profit. **You can ask them stop selling your data.**

By checking the button, we will help you to send "do not sell my data" request to data brokers. To complete the request, we need your additional information for purpose of verification.

Email

abc@hotmail.com

Do Not Sell

Figure 1: A screenshot of our browser tool's setting page. Users will need to enter their frequently used email address in the input field. After filling out the form, users only need to click the "Do Not Sell" button to attempt to opt-out of the sale of all registered data brokers. This is harder in practice than in theory.

Consumers can conveniently exercise their CCPA rights with one click. Compared with complex instructions given by companies in the registry, our tool provides a more understandable and scalable solution since consumers do not need to go to all 407 data brokers.

We notice we essentially reinvented the FTC Do Not Call list.

It would be *substantially better* if the AG's office were to host this information instead of having browser plugins and other attempt to contact data brokers and companies on the user's behalf. On the citizen side, it is better to trust the AG's office to hold PII securely than to trust browser plugins or other technologies. For companies, they would have the advantage of a single centralized list to automate checking against, rather than be pestered by random requests coming in at any time. Further, the AG's office could do a proper job of authenticating users to ensure someone is who they say they are, which benefits both citizens and companies alike. We therefore suggest the AG's office become an Authorized Agent under revised § 999.326 in providing functionality akin to the FTC's Do Not Call list.

Recommendation:

We recommend the California Attorney General's office create a centralized "Do Not Sell" database similar to the FTC's "Do Not Call" list. The Do Not Sell list would contain non-technical identifiers (such as email address, phone number, mailing address, and name,) for those who choose to join, along with notations for those protected as children.

While technical identifiers like cookies and browser fingerprints will likely be the primary way for companies to re-identify users, we do see reliance on non-technical PII in practice today on an *ad hoc* basis. The CA AG's office stepping in as an Authorized Agent under revised § 999.326 can secure consumers' rights, ease the process of exercising rights at scale, and create an automatable path for companies to ensure they are compliant with the law.

Topic 3: Tools for CCPA Compliance

Similar to our Data Guard tool, there are a few other mechanisms in development to assist users of California exercise the rights given to them by the CCPA. The most prominent is Global Privacy Control⁵. GPC utilizes an HTTP header to signal to the web server the user is interacting with that

⁵ "Privacy Badger." Electronic Frontier Foundation, [privacybadger.org/](https://www.eff.org/privacybadger/). Accessed 28 October 2020.

the user wishes to opt out of sale/share of personal data to other parties. There are several implementations of GPC, some of which we show in the figures below.



Figure 2: Privacy Badger⁶



Figure 3: Blur by Abine⁷

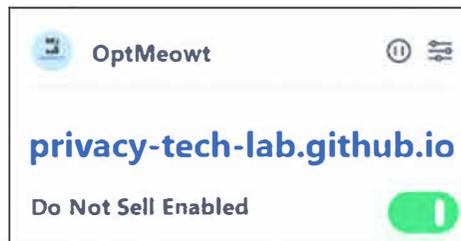


Figure 4: OptMeowt⁸

W396-4
cont

⁶ "Privacy Badger." Electronic Frontier Foundation, privacybadger.org/. Accessed 28 October 2020.

⁷ "Remove Your Personal Information From Search Engines." Abine Blur: Passwords, Payments, & Privacy, www.abine.com/. Accessed 28 October 2020.

⁸ "OptMeowt." Google, chrome.google.com/webstore/detail/optmeowt/hdbnkdbhglahihjdbodmfefogcjbpgbo. Accessed 28 October 2020.

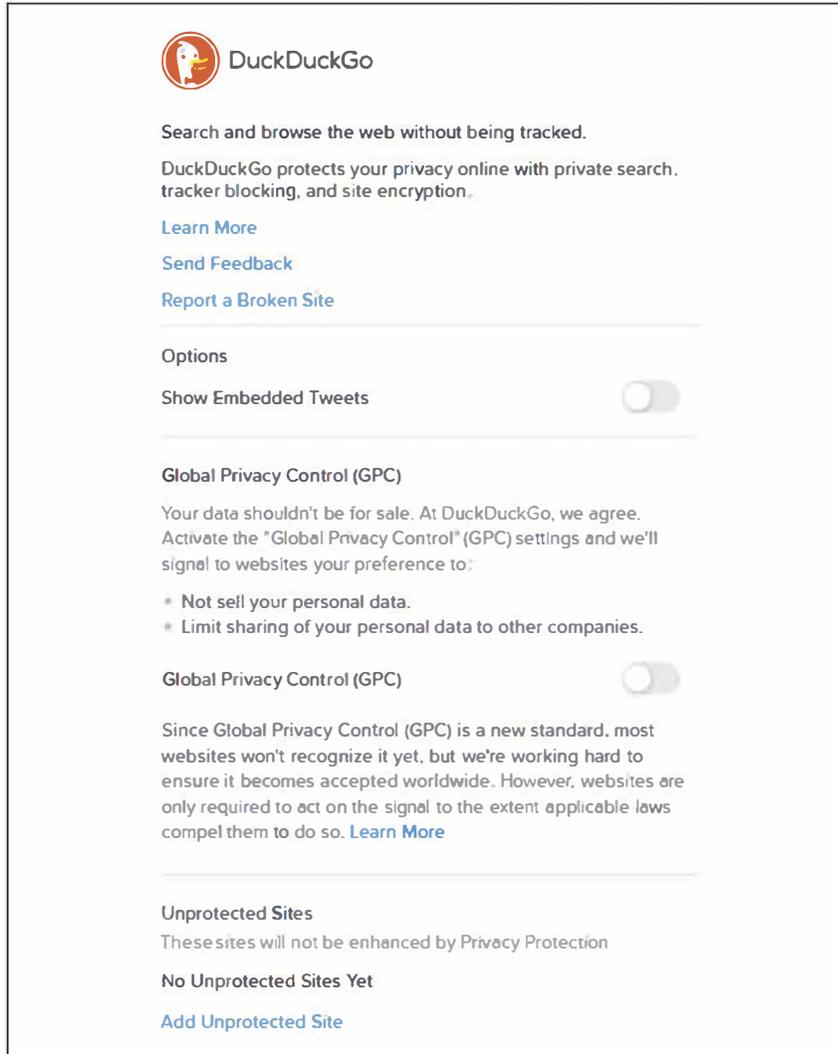


Figure 5: DuckDuckGo⁹

While these are great attempts to allow users to opt-out of sale of their data, there are concerning limitations. None of these tools appears to be responsive to age. The structure of the GPC is built upon users signaling an opt-out for the sale of data, and in the absence of the header it is assumed that they may have opted-in. This does not work for children as they must, by law, be opted out by default, including under the newly revised § 999.332. Our tool is designed to include children and teenagers. While we have great faith in the creators of GPC and assume they plan to add additional functionality later in future work, we are concerned that any early adopters may not realize the current version of GPC does not appear to be legally compliant.

The idea that some tools may be easier to use or faster is not a problem, but rather a marketplace. And indeed, GPC does some things very nicely that we do not do as well. Where we have concerns is that tools may not implement laws correctly.

⁹ Settings are enabled as described in “DuckDuckGo Founding Member in Global Privacy Control (GPC) Standards Effort,” DuckDuckGo. <https://spreadprivacy.com/announcing-global-privacy-control/>. Accessed 28 October 2020.

Recommendation:

We believe the AG’s office has an interest in ensuring tools are, at minimum, legally compliant. One light-touch way to secure that interest is to follow the prior example that led to the publication of *Privacy on the Go: Recommendations for the Mobile Ecosystem*,¹⁰ which included a series of meetings with stakeholders to develop best practice recommendations.

W396-4
cont

¹⁰ “Privacy on the Go: Recommendations for the Mobile Ecosystem,” California Office of the Attorney General (January, 2013.) https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf. Accessed 28 October 2020.

From: [REDACTED]
To: [Privacy Regulations](#)
Subject: Comment on proposed CCPA regulation revisions
Date: Friday, December 11, 2020 12:55:18 PM

§999.306(b)(3): I applaud the proposed revisions to (b)(3). This is a significant, useful clarification and is substantially less unreasonably onerous than the originally proposed language. **A welcome improvement.**

W397-1

§999.306(f): This new insertion, by contrast, is about as clear as mud, and is ill-conceived.

First, the proposed button adds nothing in terms of clarity about opt-out rights. The graphic looks like a stylized gelatin capsule covered with cryptic markings. **The average consumer is unlikely to grasp the intended significance of the graphic**, or to recognize that the button has anything to do with privacy or opting-out of the sale of their personal information.

W397-2

For consumers who use screen readers or other assistive technologies, the proposed button will be either invisible or confusing. If the graphic has an ALT tag, which WWCAG 2.0 calls for all but purely decorative images to have for accessibility purposes, the likely contents of that ALT tag would either duplicate the “Do Not Sell My Personal Information” text, which is annoying for assistive technology users, or say something different than the text (e.g., “Opt-Out”), which may be confusing and would muddle the intended clarity of the phrase “Do Not Sell My Personal Information.”

W397-3

In sum, this graphic is ugly and unhelpful; I don’t believe that the button is in any way clearer than the phrase “Do Not Sell My Personal Information” that is already separately required; and for vision-impaired users, it may actually be LESS clear.

W397-2
and
W397-3

Second, **the wording of this provision makes it unclear if use of the proposed button is intended to be mandatory:** (f)(1) suggests that it is optional (“may be used in addition to posting”), while (f)(2) implies that it MUST be used in addition to and as part of any Do Not Sell My Personal Information link (“Where a business ... shall be added”). I am genuinely uncertain which interpretation your office intends, which is a bad choice for a regulation intended to “promote consumer awareness.”

W397-4

I would strongly oppose any move to make this ugly, ill-conceived button graphic mandatory as part of the already-required Do Not Sell My Personal Information (DNSMPI) link. In addition to the points noted above, use of the graphic may be impractical or infeasible in a variety of contexts where the link might reasonably be presented — for example, in a bullet-pointed list in a sidebar menu on a web page, or in the footer of an email message. (Not all email clients support the use of graphics within the body or footer of an email message, so the graphic would simply be stripped out in plain-text messages anyway.) Furthermore, since (f)(1) does make clear that the button must be used in addition to the phrase “Do Not Sell My Personal Information,” adding the button would

W397-5

exacerbate the problem with fitting the link's required anchor text into space-restricted contexts (such as on the settings menu of mobile app or in the narrow sidebar of a website template intended for mobile users) without making it unreadably small or partly cut off. That would serve no one.

W397-5
cont

Making such a button mandatory would also present yet another arbitrary technical headache for businesses that have already made a good-faith effort to comply with the regulatory requirements. (Indeed, I would question OAG's good faith in promulgating an additional compliance requirement in a set of regulatory revisions that will be seen only by a limited audience and which has a public comment period of only 18 calendar days.)

W397-6

If the intent is simply to make this graphic (or some hopefully less ugly and less cryptic variant) optional, or optional and encouraged, the proposed text should make that clearer.

§999.315(h): I was dismayed and disheartened to see that OAG has made no attempt whatever to address the problems I previously broached with regard to this proposed addition.

First, let me reiterate that I appreciate the overall intent of this section to discourage businesses from "burying" their opt-out requirements or obfuscating them with confusing language. I don't have a fundamental problem with that goal.

That said, several of the specific provisions OAG has inserted create a series of confusing, arbitrary, impractical, and ultimately unenforceable requirements, which remain unchanged in the current revision.

First among these is §999.315(h)(1), which seeks to impose a specific arbitrary standard for the acceptable number of steps or clicks to opt-out. **This is frankly nonsensical, particularly in view of the additional requirements created by the proposed §999.306(b)(3).** Consider: a brick-and-mortar business such as a grocery store, which sells personal information gathered from consumers in the store in connection with the use of a store "club card." Opting-in may be as simple as taking the new card from an employee and swiping it at the POS terminal. The process of subsequently opting-out would certainly require more steps than that; at a minimum, the consumer would need to provide their club card number (so that the opt-out request is correctly applied to their account) and then indicate their desire to opt-out by pressing or otherwise indicating the desired option.

W397-7

Similarly, consider a web-based business that runs online advertising and also collects logged-in visitors' email addresses for a mailing list that is also sold to third parties. The online advertising is configured to respond to Global Privacy Control browser settings, so that visitors who send an opt-out signal are not shown advertising that collects personal information, while logged-in visitors can separately opt-out of the sale of their email addresses. In the first case, the visitor's opt-in or opt-out preference is communicated by the browser signal, which requires no clicks at all, and may not provide the website with enough information to individually identify that visitor. In the second case, the visitor would reasonably need to submit an opt-out request that provides their name and email address so that the business may correctly process the request. Under the proposed 999.315(h)(5), the business would be expected to enable consumers to submit the second type of opt-out request using no more clicks than the first (which in this example would be no clicks at all). **That's obviously**

absurd, and completely impracticable.

Again, I recognize and appreciate the desire to discourage opt-out procedures that require an unreasonable number of steps, but the way this provision is worded and its ludicrous demand for parity in situations that are clearly not directly equivalent suggests that whoever wrote this proposed §999.315(h)(1) has simply not thought through the onerous and confusing expectations it creates. I think you're trying to square the circle here, and I see no way to revise this subparagraph to achieve your desired end without the ridiculous and unreasonable problems the present version creates. **I still believe §999.315(h)(1) should be deleted in its entirety from these proposed revisions.**

The other absurd and arbitrary provision here remains §999.315(h)(5), which seeks to require that a consumer not have to "scroll or search" through a webpage to find opt-out instructions.

As I expressed in my previous public comment, I appreciate that the intent is to discourage "burial" of the opt-out instructions, but the wording you've proposed would have the effect of *prohibiting* ANY scrolling, which again is absurd. How much scrolling may be required to reach specific text on a given webpage is directly dependent on the dimensions of the user's browser window, monitor, or mobile device screen, which is completely outside the control of the website's operators. **Even if a business has a separate Do Not Sell My Personal Information page containing clear, reasonably concise instructions for submitting an opt-out request, reaching those instructions may require some scrolling if the page is accessed on a mobile phone.** To the person who wrote this paragraph, I must ask: How big is YOUR phone's screen? My own mobile device has a screen size of 5 inches, measured diagonally (and my previous phone's screen was smaller still), so many webpages that would require little or no scrolling or searching on my desktop will have me scrolling madly away when accessed from my phone. Even on a desktop, if I reduce the size of my browser window and/or enlarge the text for easier reading, it will significantly increase the amount of scrolling involved in reading a particular page or section of a page, even a short one.

That's beyond the control of the websites I visit, and it doesn't necessarily connote any bad faith on their part as regards these regulations; it is simply a plain reality of the physical dimensions of Internet-capable devices and web browsers. Under this proposed rule, such a website would be in technical violation of these regulations and could be legally penalized for it — madness! Similarly, a business could be penalized for technical errors, such as an anchor link that fails to correctly resolve, which is not at all reasonable.

My objections to §999.315(h)(5) could be mitigated through the addition of qualifiers such as "to an excessive or unreasonable degree" to the proposed text. (What is "unreasonable" or "excessive" is obviously a subjective judgment, but so is most of the proposed §999.315(h).) Failing that, 315(h)(5) should be deleted in its entirety. Once again, I understand what you're trying to achieve here, but the writer(s) of this section have not considered the implications of the often-clumsy wording.

I sincerely hope that this time, OAG will take these concerns into consideration prior to finalizing the proposed revisions.

W397-7
cont

[REDACTED]

[REDACTED]

[REDACTED]

From: [Maureen Mahoney](#)
To: [Privacy Regulations](#)
Subject: CR Comments on Fourth Set of Modifications to the CCPA Regulations
Date: Wednesday, December 23, 2020 10:07:33 AM
Attachments: [CR Comments on 4th Set of Modifications to the CCPA.pdf](#)

Hello,

Attached, please see Consumer Reports' comments on the Fourth Set of Modifications to the CCPA Regulations. Please let me know if you have any questions.

Best,
Maureen

--

Maureen Mahoney, Ph.D.

Policy Analyst

m [REDACTED]

Pronouns: she/her/hers

[CR.org](#)



This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.



December 23, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Fourth Set of Modifications to Regulations Implementing the California Consumer Privacy Act (CCPA)

Dear Ms. Kim,

Consumer Reports¹ appreciates the opportunity to comment on the Fourth Set of Modifications to the CCPA Regulations.² We thank the California Attorney General’s office (AG) for proposing new regulations to help to make the CCPA work better for consumers. Though the California Consumer Privacy Act (CCPA) is designed to protect consumer privacy, Consumer Reports has found that some consumers ran into difficulties when attempting to opt out of the sale of their information under the CCPA.³ The new proposed rules will help address some—though not all—of these problems. To better ensure that consumers are able to exercise their privacy rights, we reiterate our comments submitted in response to the Third Set of Modifications (attached),⁴ and additionally, recommend that the AG:

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

² California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Dec. 10, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-prop-mods-text-of-regs-4th.pdf>.

³ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?*, CONSUMER REPORTS DIGITAL LAB (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

⁴ Maureen Mahoney, Consumer Reports Comments on the Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act (Oct. 28, 2020), <https://advocacy.consumerreports.org/research/cr-comments-on-the-third-set-of-modifications-to-proposed-regulations-implementing-the-ccpa/>.

- Finalize the proposed opt-out button design;
- More clearly require companies that sell personal information to include the opt-out button on their homepages, along with the “Do not Sell My Personal Information” link;
- Clarify that if an authorized agent inadvertently submits a request incorrectly, the company must either accept it or inform the agent how to submit it appropriately; and
- Clarify the definition of sale and tighten the restrictions on service providers, to ensure that consumers can opt out of cross-context targeted advertising.

See Below

Consumers’ activity online is constantly tracked, and information about their most personal characteristics sold without their knowledge or consent. At the very least, consumers should be able to effectively opt out of the sale of their personal information to third parties. The following reforms, if adopted, will better ensure that consumers are able to do so.

The AG should finalize the proposed opt-out button design.

Consumer Reports has documented that consumers often find it difficult to locate Do Not Sell links on data brokers’ homepages. In our recent study, *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?*, over 500 consumers submitted Do Not Sell requests to approximately 200 companies on the California Data Broker Registry. Each company was tested by at least three study participants. We found that for 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a “Do Not Sell” link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.

In some cases, the opt-out links simply weren’t there; in others, the links were difficult to find. Follow-up research focused on the sites in which all three testers did not find the link revealed that at least 24 companies on the data broker registry did not have the required DNS link on their homepage. All three testers were unable to find the DNS links for five additional companies, though follow-up research revealed that the companies did have DNS links on their homepages. Still, this also raised concerns, since the CCPA requires companies to post the link in a “clear and conspicuous” manner.⁵ If consumer testers who are actively searching for DNS links have difficulty finding them on the homepage, it’s hard to imagine that the everyday consumer will find them.

W398-1

Thus, we recommend that the AG finalize the opt-out button design as proposed. We appreciate the work that went into developing the opt-out button, which reflects the design and approach recommended by Professor Lorrie Cranor and her colleagues, based on their research.⁶ The

⁵ Cal. Civ. Code §1798.135(a)(1).

⁶ Lorrie Faith Cranor et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* at 32 (Feb. 4, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cranor-design-eval-usable-icon.pdf>.

proposed opt-out button should help draw the consumer’s eye to the Do Not Sell link.⁷ After the button is adopted and placed on homepages, we urge the AG’s office to continue to work with researchers, academics, advocacy organizations, and companies in evaluating the efficacy of the design and update if needed to ensure that it is useful for consumers.

W398-1
cont

The AG should more clearly require companies that sell personal information to post the opt-out button on their homepages, along with the “Do not Sell My Personal Information” link.

Unless use of the button is required, it is unlikely that enough companies will adopt it. We therefore appreciate that the AG has proposed to require companies that sell personal information to post the opt-out button alongside the “Do Not Sell My Personal Information” link on the homepage.⁸ But while we think it is clear that the proposed language in §999.306(f)(1)-(3) requires companies selling personal information to post the button on their homepages, some observers have a different interpretation, that posting of the button is optional.⁹ An optional interface would counter the direct instructions in the CCPA, for the AG to issue rules “For the development and use of a recognizable and uniform opt-out logo or button *by all* businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.”¹⁰ [emphasis added]

W398-2

To help eliminate any uncertainty that the opt-out button is required, we propose the following tweak to the proposed language:

f) Opt-Out Button. (1) The following opt-out button ~~may~~ shall be used in addition to posting the notice of right to opt-out, ~~but~~ and not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations. (2) Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button shall be added to the left of the text as demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link. (3) The button shall be approximately the same size as any other buttons used by the business on its webpage.

Without more clearly establishing that use of the opt-out button is required on the homepage, it is likely that companies will disregard it. Standardized notice is important to making CCPA

⁷ Lorrie Faith Cranor et al., *CCPA Opt-Out Icon Testing - Phase 2* at 2, 23 (May 28, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/dns-icon-study-report-052822020.pdf>.

⁸ Text of Modified Regulations, *supra* note 2, at §999.306(f)(1)-(3).

⁹ See, eg, @JulesPolonetsky, Twitter (Dec. 10, 2020), <https://twitter.com/JulesPolonetsky/status/1337116699548667907>.

¹⁰ Cal. Civ. Code § 1798.185(a)(4)(C).

disclosures meaningful for consumers. And widespread adoption of the button should better ensure that consumers can more easily opt out of the sale of their personal information.

W398-2
cont

The AG should clarify that if an authorized agent inadvertently submits a request incorrectly, the company must either accept it or inform the agent how to submit it appropriately.

The CCPA’s authorized agent provisions, which allow consumers to designate an authorized agent to submit access, deletion, and opt-out requests on their behalf, are crucial to making the CCPA more workable for consumers.¹¹ Instead of submitting hundreds, if not thousands of requests to different companies in order to exercise their privacy preferences, which could end up taking almost as much time as a full-time job, the consumer can simply delegate authority to a third party. Consumer Reports, seeking to help make it easier for consumers to exercise their CCPA rights, has been conducting a study of the authorized agent provision and has submitted opt-out requests on behalf of about one hundred California consumers.¹² (We expect to publish the results of our findings early next year).

W398-3

Our research has shown that some companies do not clearly describe in their privacy policies the correct methods to submit authorized agent requests—as is required by the CCPA regulations.¹³ It can be difficult for the authorized agent to know the company’s preferred process, creating uncertainty as to whether the requests have been honored.

To help address this problem, the AG should require that when an authorized agent inadvertently submits a request through a method not accepted by the company, that the company shall either accept the request or instruct the authorized agent with the correct method of submission. The AG regulations already require companies to treat consumers’ verifiable requests in this manner;¹⁴ these protections should be extended to authorized agents, for all requests.

The AG should clarify the definition of sale and tighten the restrictions on service providers, to ensure that consumers can opt out of cross-context targeted advertising.

Finally, in the course of submitting opt-out requests on behalf of consumers, we learned about more companies that claimed that they did not “sell” information under the CCPA, though they shared it with third parties for cross-context targeted advertising.

W398-4

¹¹ Cal. Civ. Code § 1798.135(a)(1); § 1798.185(a)(7).

¹² Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, Digital Lab at Consumer Reports (Oct. 19, 2020),

<https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8>.

¹³ Cal. Code Regs. tit. 11 § 999.308(c)(5) (2020).

¹⁴ *Id.* at 999.312(e).

We reiterate the request from our previous comments to clarify that these data transfers are covered by the CCPA's definition of sale,¹⁵ and to close up exemptions in the service provider exemption that companies have exploited.¹⁶ The CCPA places next to no restrictions on first-party collection and use of data, but it seeks to give consumers control over third-party use of their personal information without their permission. The newly-passed California Privacy Rights Act (CPRA) removes all doubt that these transfers are covered,¹⁷ but those provisions will not go into effect for another two years.¹⁸ Consumers should not have to wait two more years to be able to adequately protect their privacy. We urge the AG to close the loopholes in the definition of sale and service provider without delay.

W398-4
cont

Conclusion

Thank you for the opportunity to comment on the Fourth Set of Proposed Modification to the CCPA. Please do not hesitate to reach out if you have any questions.

Respectfully submitted,



Maureen Mahoney
Policy Analyst

Attachment

¹⁵ Consumer Reports Comments on the Third Set of Modification to Proposed Regulations Implementing the California Consumer Privacy Act, *supra* note 4, at 7.

¹⁶ *Id.* at 8-9.

¹⁷ See, California Privacy Rights Act, § 1798.120(a); § 1798.140(e)(6), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

¹⁸ *Id.* at § 1798.185(d).



October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act (CCPA)

Dear Ms. Kim,

Consumer Reports¹ appreciates the opportunity to submit comments in response to the Notice of the Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act.² We welcome these proposed changes, especially those prohibiting the use of dark patterns—methods that substantially interfere with consumers’ efforts to opt out of the sale of their information.³ Consumer Reports has recently documented that some consumers are finding it very difficult to opt out of the sale of their information.⁴ In our recent study, over 500 consumers submitted opt-out requests to companies listed on the California data broker registry. Many of them encountered challenges: opt-out links too often were missing from the home page or difficult to find; opt-out processes were unnecessarily complicated, and companies asked consumers to submit sensitive information to verify their identities. In response, consumers sent over 5,000 messages to the AG, urging him to step up enforcement efforts and close up

W398-5

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

² California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Oct. 12, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf>.

³ *Id.* at §999.315(h)(1)-(5).

⁴ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers’ Rights Protected?*, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

loopholes in the CCPA that companies have exploited. The guidance on opt outs, including the prohibition on dark patterns, in this latest proposal will go a long way to addressing these problems. But more work is needed to ensure that consumers can properly exercise their privacy rights. We recommend that the AG:

- Finalize the proposed guidance on opt outs, including the prohibition on dark patterns;
- Finalize a design for the opt-out button;
- Require companies to confirm that they have honored opt-out requests;
- Finalize the authorized agent provisions as proposed;
- Close up loopholes in the definition of sale and tighten protections with respect to service providers, to ensure that consumers can opt out of behavioral advertising;
- Clarify that financial incentives in markets that lack competition is an unfair and usurious practice; and
- Establish a non-exclusive list of browser privacy signals that shall be honored as a universal opt out of sale.

Below, we explain these points in more detail.

The AG should finalize the proposed guidance on opt outs, including the prohibition on dark patterns.

We appreciate that the AG has proposed to “require minimal steps to allow the consumer to opt-out” and to prohibit dark patterns, in other words, “a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer’s choice to opt-out.”⁵ These regulations are essential given the difficulties that consumers have experienced in attempting to stop the sale of their information.

Subverting consumer intent online has become a real problem, and it’s important to address. In response to Europe’s recent GDPR privacy law, many websites forced users through confusing consent dialogs to ostensibly obtain consent to share and collect data for any number of undisclosed purposes.⁶ And researchers increasingly have been paying attention to manipulative dark patterns as well. A 2019 Princeton University study of 11,000 shopping sites found more than 1,800 examples of dark patterns, many of which clearly crossed the line into illegal deception.⁷

⁵ § 999.315(h).

⁶ *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

⁷ Mathur, Arunesh and Acar, Gunes and Friedman, Michael and Lucherini, Elena and Mayer, Jonathan and Chetty, Marshini and Narayanan, Arvind, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. (2019), <https://webtransparency.cs.princeton.edu/dark-patterns/>.

Use of these dark patterns is already illegal under Unfair and Deceptive Acts and Practices (UDAP) law, but that hasn't been adequate to protect consumers from these deceptive interfaces. For example, the Federal Trade Commission (FTC) sued Age of Learning, an online education service for children, for its deceptive interface that led consumers to believe they were signing up for one year of service, when in fact, by default, they were charged each year.⁸ Attorney General Karl Racine of the District of Columbia recently filed suit against Instacart for using a deceptive interface that made a service fee look like a tip.⁹ Last year, the FTC alleged that Match.com tricked consumers into subscribing by sending them misleading advertisements that claimed that someone wanted to date them—even though many of those communications were from fake profiles.¹⁰ Similarly, in late 2016, the FTC took action against Ashley Madison for using fake profiles to trick consumers into upgrading their membership.¹¹ The FTC took action against Facebook in 2011 for forcing consumers to use a deceptive interface to get them to provide so-called “consent” to share more data.¹² Despite these enforcement actions, the use of dark patterns remains all too common. Given how widespread these interfaces are, it's important to explicitly clarify that they are illegal in the CCPA context.

The proposed rules appropriately rein in the number of allowable steps to opt out.

We appreciate that the proposed rules limit the number of allowable steps in the opt-out process.¹³ As we noted in our recent study, some “Do Not Sell” processes involved multiple, complicated steps to opt out, including downloading third-party software, raising serious questions about the workability of the CCPA for consumers. For example, the data broker Outbrain doesn't have a “Do Not Sell My Personal Information” link on its homepage. The

⁸ Fed. Trade Comm'n v. Age of Learning, Inc., Complaint for Permanent Injunction and Other Equitable Relief, Case No. 2:20-cv-7996. U.S. District Court Central District of California at 4-6 (Sept. 1, 2020), <https://www.ftc.gov/system/files/documents/cases/1723086abcmousecomplaint.pdf>. According to the FTC, this is a UDAP violation, *See* ¶ 57.

⁹ District of Columbia v. Maplebear, Inc. d/b/a Instacart, Complaint for Violations of the Consumer Protection Procedures Act and Sales Tax Law, Superior Court of the District of Columbia at ¶ 2 (Aug. 2020), <https://oag.dc.gov/sites/default/files/2020-08/Instacart-Complaint.pdf>. The AG alleged that “Instacart’s misrepresentations and omissions regarding its service fee constitute deceptive and unfair trade practices that violated D.C. Code § 28-3904.” *See* ¶ 86.

¹⁰ Fed. Trade Comm'n v. Match Group, Inc., Complaint for Permanent Injunction, Civil Penalties, and Other Relief, Case No. 3:19-cv-02281, U.S. District Court, Northern District of Texas, Dallas Division at 2 (Sept. 25, 2019), https://www.ftc.gov/system/files/documents/cases/match_-_complaint.pdf. According to the FTC, this is a Section 5 violation. *See* p. 20-21.

¹¹ Fed. Trade Comm'n v. Ruby Corp. et al, Complaint for Permanent Injunction and Other Equitable Relief, Case 1:16-cv-02438, United States Circuit Court for the District of Columbia at 6 (Dec. 14, 2016), (<https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf>). According to the FTC, this is a Section 5 violation. *See* p. 13-14.

¹² Fed. Trade Comm'n, In the Matter of Facebook Inc. at 5-6 (2011) <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>. According to the FTC, this is a Section 5 violation. *See* p. 19.

¹³ § 999.315(h)(1).

consumer can click on the “Privacy Policy” link at the bottom of the page, which sends the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer can cut out several steps by clicking on “Interest-Based Ads” on the homepage.) If a consumer would like to opt out on their phone, they would have to go through another process. And if the consumer clears their cookies, they would need to opt out again. As one consumer told us, “It was not simple and required reading the ‘fine print.’” The proposed rules should help address this problem.

The proposed rules correctly prohibit companies from asking for unnecessary information to opt out.

We also appreciate the guidance that opt-out processes “shall not require the consumer to provide personal information that is not necessary to implement the request.”¹⁴ In our study, participants reported that they gave up the opt-out request 7% of the time. The overwhelming reason for a consumer to refrain from part of a DNS request process, or give up all together, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: “I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty.” Even consumers that ended up providing the drivers’ license ended up confused by the company’s follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: “After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that ‘[w]e will update the ranges in the future release.’ I have no idea what that means.” Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.

This information is clearly not necessary, as most data brokers simply requested name, address, and email. Unnecessary collection of sensitive data has significantly interfered with consumers’ ability to exercise their rights under the CCPA, and we appreciate that the proposed rules explicitly prohibit this.

¹⁴ § 999.315(h)(4).

The draft rules correctly stop businesses for making consumers search through a privacy policy to opt out.

We are also pleased that the draft rules preclude businesses from requiring consumers to dig through privacy policies to opt out.¹⁵ In our study, in some cases, consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, “There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart.” Another said of Oracle America, “The directions for opting out were in the middle of a wordy document written in small, tight font.” Another found the legal language used by Adrea Rubin Marketing intimidating: “they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury.”

Another data broker, ACBJ, placed a “Your California Privacy Rights” link at the bottom of their homepage (rather than a “Do Not Sell My Personal Information” link), which led to their privacy and cookie policy.¹⁶ Once on the policy page, the consumer is forced to search in their browser for the phrase “Do Not Sell My Personal Information” or scroll and scan ten sections of the privacy policy to find the paragraph with a “Do Not Sell My Personal Information” link, or follow two additional links to navigate from the privacy policy table of contents to the “Do Not Sell My Personal Information” link. Upon clicking the “Do Not Sell My Personal Information” link, the consumer is shown a pop-up with a page of additional legal information, and then has to scroll down to a toggle that finally allows them to request their data not be sold. In light of these reports from consumers, we urge the AG to finalize the prohibition on these practices.

The AG should finalize a design for the opt-out button.

Given that many consumers found it difficult to find the Do Not Sell link—it was often labeled with something different, and often buried at the bottom of the page with other links—a standardized graphic button would likely have value in ensuring that consumers would take advantage of that privacy protection. The CCPA directs the AG to design an opt-out button: “a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.”¹⁷ While the original design came under a fair amount of criticism, a uniform button will likely help consumers seeking to opt out, and the AG should promulgate one as soon as possible.

¹⁵ § 999.315(h)(5).

¹⁶ ACBJ (last visited Oct. 28, 2020), <https://acbj.com/privacy#X>.

¹⁷ Cal. Civ. Code § 1798.185(a)(4)(C).

The AG should require companies to confirm that they have honored opt-out signals.

In our study, many consumers had no idea whether or not their opt-out request had been honored. The uncertainty often left consumers dissatisfied with the opt out. Some companies did notify consumers that their requests had been honored, and this information was characteristic of simple, quick, and effective opt-out processes.

Only in 18% of requests did participants report a clear confirmation from the broker that their data was or would soon not be sold. In 46% of tests, participants were left waiting or unsure about the status of their DNS request. In the 131 cases where the consumer was still waiting after one week, 82% were dissatisfied with the process (60% reported being very dissatisfied, and 22% reported being somewhat dissatisfied). The lack of clarity and closure was reflected in consumer comments such as “left me with no understanding of whether or not anything is going to happen” and “While it was an easy process—I will read their privacy policy to see if there is more [I] have to do to verify they are complying with my request. They left me unsure of the next step.”

The AG should approve the proposed adjustment to the authorized agent provisions.

The authorized agent provisions are an essential part of the CCPA, and Consumer Reports has recently launched a pilot program to perform opt-out requests on consumers’ behalf.¹⁸ The CCPA puts far too much burden on individuals to safeguard their privacy; being able to designate an authorized agent to act on consumers’ behalf can help reduce that burden. The draft regulations support the work of authorized agents submitting access, deletion, and opt-out requests on consumers’ behalf, while ensuring that consumers’ privacy and security is protected.

While the CCPA pointedly does not require identity verification for opt-out requests, access and deletion requests have strong identity verification requirements. The regulations make it appropriately clear that a business may require additional identity verification, but not if the authorized agent can present proof that it holds a power of attorney from the consumer.¹⁹ If multiple companies required a consumer to submit additional identity verification, the authorized agent provision would no longer be practical for consumers. Obtaining a single power of attorney is easier and more efficient than going through many identity verification steps. Industry standards and standard form powers of attorney will make access and deletion pragmatic for the consumer, like the authorized agent opt-out process is currently.

¹⁸ Ginny Fahs, *Putting the CCPA Into Practice: Piloting a CR Authorized Agent*, DIGITAL LAB AT CONSUMER REPORTS (Oct. 19, 2020), <https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8>.

¹⁹ § 999.326(b)

W398-5
cont

The regulations also require companies to honor valid opt-out requests from an authorized agent unless they have a “good-faith, reasonable, and documented belief that a request to opt-out is fraudulent.”²⁰ With these guidelines, an authorized agent that uses industry-standard verification of a consumer’s email address or telephone number will be able to complete an opt out without requiring consumers to provide hundreds, if not thousands, of verifications. This language allows companies to reject fraudulent opt outs without putting additional verification burdens on a consumer using a legitimate authorized agent.

The AG should clarify the definition of sale and tighten protections with respect to service providers, to ensure that consumers can opt out of behavioral advertising.

Many tech companies have exploited ambiguities in the definition of sale and the rules surrounding service providers to ignore consumers’ requests to opt out of behavioral advertising.²¹ Companies such as Spotify and Amazon claim that they are not “selling” data and that consumers can’t opt out of these data transfers—even though they share it with their advertising partners.²² Some companies claim that because data is not necessarily transferred for money, it does not constitute a sale.²³ But addressing targeted advertising is one of the main goals of the CCPA, which has an inclusive definition of personal information and a broad definition of sale to cover transfers of data for these purposes.²⁴

Given the extent of the non-compliance, the AG should exercise its broad authority to issue rules to further the privacy intent of the Act,²⁵ and clarify that the transfer of data between unrelated companies for any commercial purpose falls under the definition of sale. This will help ensure that consumers can opt out of cross-context targeted advertising. We suggest adding a new definition to § 999.301:

“Sale” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s

²⁰ § 999.315(g)

²¹ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, DIGITAL LAB AT CONSUMER REPORTS (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>.

²² Spotify, “Additional California Privacy Disclosures,” (July 1, 2020), <https://www.spotify.com/us/legal/california-privacy-disclosure/?language=en&country=us>; Amazon.com Privacy Notice,” (January 1, 2020), https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40_SECTION_FE2374D302994717AB1A8CE585E7E8BE.

²³ Tim Peterson, *‘We’re Not Going to Play Around’: Ad Industry Grapples with California’s Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), <https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/>.

²⁴ Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>; Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(t).

²⁵ Cal. Civ. Code § 1798.185(a).

personal information by the business to another business or a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

Another common way for companies to avoid honoring consumers' right to opt out of behavioral advertising is by claiming a service provider exemption. For example, the Interactive Advertising Bureau (IAB), a trade group that represents the ad tech industry, developed a framework for companies to evade the opt out by abusing a provision in the CCPA meant to permit a company to perform certain limited services on its behalf.²⁶

To address this problem, the AG should clarify that companies cannot transfer data to service providers for behavioral advertising if the consumer has opted out of sale. We reiterate our calls for a new .314(d):

If a consumer has opted out of the sale of their data, a company shall not share personal data with a service provider for the purpose of delivering cross-context behavioral advertising. "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

Additionally, the AG should take action to stop companies from combining data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they're just service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets. The AG has appropriately removed language in an earlier draft, which held that service providers can merge data across clients. But in the absence of a specific prohibition, given its disregard for the FTC consent order, Facebook (and other companies) will likely continue to engage in this behavior. The AG needs to make clear that this is not acceptable. We suggest the following language:

A service provider may not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

²⁶ *IAB CCPA Compliance Framework for Publishers & Technology Companies*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf.

Google and Facebook provide app developers privileged, valuable information—your data—in return for services that help increase engagement with their platforms.²⁷ The AG should refine the regulations in order to give consumers more control over their data with respect to these practices.

The AG should clarify that financial incentives in markets that lack competition is an unfair and usurious practice.

Californians have a right to privacy under the California Constitution, and consumers shouldn't be charged for exercising those rights. Unfortunately, there is contradictory language in the CCPA that could give companies the ability to charge consumers more for opting out of the sale of their data or otherwise exercising their privacy rights.²⁸

To prevent some of the worst abuses associated with financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The CCPA prohibits financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.²⁹ And, the AG currently has the authority under the CCPA to issue rules with respect to financial incentives.³⁰ Thus, we urge the AG to exercise its authority to prohibit the use of financial incentives in market sectors that lack competition. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates—about \$30 per month—for not leveraging U-Verse data for ad targeting.³¹ Where consumers have few choices, market forces don't impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,³² further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.³³ The AG should exercise its authority to put reasonable limits on these programs in consolidated markets.

W398-5
cont

²⁷ Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.

²⁸ Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).

²⁹ *Id.* at § 1798.125(b)(4).

³⁰ *Id.* at § 1798.185(a)(6).

³¹ Jon Brodtkin, *AT&T To End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), <https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/>.

³² *Too Much of a Good Thing*, THE ECONOMIST (March 26, 2016), <https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing>.

³³ *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets*, Fed. Trade Comm'n (Feb. 26, 2019), <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology>.

The AG should clarify a non-exclusive list of browser privacy signals that shall be honored as a universal opt out of sale.

We appreciate that the AG has maintained the requirement that companies must honor browser privacy signals as an opt out of sale.³⁴ Forcing consumers to opt out of every company, one by one is simply not workable. However, the current rules should be adjusted to ensure that it is consumer-friendly. The AG should state that platform-level controls to limit data sharing should be interpreted as CCPA opt outs, including Do Not Track and Limit Ad Tracking. Or at the very least, the AG should clarify how platforms can certify that new or existing privacy settings should be construed as CCPA opt outs.

To encourage the development and awareness of, and compliance with, privacy settings for other platforms, we reiterate our request that the AG to issue rules governing: 1) how the developer of a platform may designate a particular privacy control to be deemed a valid request; 2) how the attorney general shall maintain and publish a comprehensive list of privacy controls to be deemed valid requests; and 3) the conditions under which business may request an exception to sell data notwithstanding a consumer’s valid request.

Millions of consumers have signed up for Do Not Track, but there are other settings that are far less well-known, in part because they’re not associated with online use. For example, Apple, in 2013 introduced a mandatory “Limit Ad Tracking” setting for iPhone applications, and recently improved that tool to further limit the information advertisers can receive when the setting is activated.³⁵ Consumers also need global opt outs from sale when using their smart televisions and voice assistants. In order to better raise awareness of the different options on the market, to encourage the development of new tools, and to address the lack of clarity around which browser settings must be honored as opt outs, the AG should set up a system in order to make this clear for consumers and businesses.

Additionally, it would be helpful to provide guidance outside of the rule that signals such as the Global Privacy Control—a new, CR-supported effort to create a “Do Not Sell” browser signal³⁶—are likely to be considered binding in the future.

Conclusion

The proposed rules, particularly the guidance on opt-out requests, will help rein in some of the worst abuses of the opt-out process. But more needs to be done in order to ensure that the CCPA

³⁴ § 999.315(c).

³⁵ Lara O’Reilly, *Apple’s Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You*, BUS. INSIDER (Sept. 10, 2016), <http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9>.

³⁶ Press release, *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights*, Global Privacy Control (Oct. 7, 2020), <https://globalprivacycontrol.org/press-release/20201007> html.

W398-5
cont

is working as intended. We look forward to working with you to ensure that consumers have the tools they need to effectively control their privacy.

W398-5
cont

Respectfully submitted,

Maureen Mahoney
Policy Analyst
Consumer Reports

From: [Steven K. Hazen](#)
To: [Privacy Regulations](#)
Subject: OAL File No. 2019-1001-05 (comment on Fourth Set of Proposed Modifications to Text of CCPA Regulations)
Date: Wednesday, December 23, 2020 8:30:14 PM
Attachments: [SKHazen Comment on 4th Proposed Regs CCPA \(Dec 23 2020\).pdf](#)

Attached: comment letter by Steven Kelsey Hazen addressing the above referenced announcement and rule making by the Department of Justice.

Steven Kelsey Hazen, Esq.
149 South Barrington Avenue, #245
Los Angeles, CA 90049-3310

December 23, 2020

VIA EMAIL: PRIVACYREGULATIONS@DOJ.CA.GOV

Lisa B. Kim, Esq.
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

re Fourth Set of Proposed Modifications to Text of CCPA Regulations
OAL File No. 2019-1001-05

Dear Ms. Kim:

This letter is provided in response to the announcement dated December 10, 2020 of the above-referenced proposed modifications to Regulations promulgated by the Department of Justice pursuant to the California Consumer Privacy Act (the “CCPA”). In that context, I draw your attention to the text of proposed new section (f) of § 999.306 (“Notice of Right to Opt-Out of Sale of Personal Information”). Specifically, there appears to be some confusion as between part (1) and parts (2) and (3), or even contradiction of the former by the latter.

The proposed text of part (1) makes it clear that use of the identified “button” is voluntary: it “may be used in addition to posting the notice of right to opt-out, but not in lieu of ...” complying with requirements of Civil Code section 1798.135 and the regulation implemented under the CCPA. By contrast, the proposed text of parts (2) and (3) might be understood as making use of such button mandatory: “the button shall be added ...” [part (2)]; “button shall be approximately the same size ...” [part (3)]. In each case, the underlining in the quoted text is added for purposes of highlighting the comparison.

In order to be consistent with the provisions of part (1), I suggest that part (2) be modified so that reference in the first sentence of it to “the opt-out button” instead read as follows: “the opt-out button (if used)”. Similarly, I suggest that the first four words of part (3) currently reading “The button shall be” instead read as follows: “The button (if used) shall be”. Making these changes will avoid potential confusion by parties subject to the provisions of the CCPA and the Regulations adopted under them.

Respectfully submitted,

/s/
Steven Kelsey Hazen

W399-1

From: [Dylan Hoffman](#)
To: [Privacy Regulations](#)
Subject: Internet Association Comments on Fourth Modified CCPA Regulations
Date: Thursday, December 24, 2020 7:47:02 AM
Attachments: [IA Comments on 4th Modified CCPA Regs 12.24.20.pdf](#)

Hi,

Please find attached comments from Internet Association on the Third Modified CCPA Regulations. If you have any questions please let me know.

Best,

--



Dylan Hoffman

Director of California Government Affairs



INTERNET ASSOCIATION

1303 J Street, Suite 400, Sacramento, CA 95814



December 24, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Internet Association (“IA”) appreciates the opportunity to review and provide the Attorney General’s Office (“AGO”) feedback on the Text of Modified Regulations for the California Consumer Privacy Act (“CCPA”) Regulations (“Modified Regulations”). IA is the only trade association that exclusively represents leading global internet companies on matters of public policy.¹ Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society, and as the voice of the world’s leading internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits. IA members are committed to providing consumers with strong privacy protections and control over personal information, as well as to compliance with applicable laws, and advocates for a modern privacy framework in the IA Privacy Principles.² Internet companies believe individuals should have the ability to access, correct, delete, and download data they provide to companies both online and offline.

IA hopes to continue working with the AGO’s office to clarify these regulations. We are encouraged by some of the recent proposals in the latest Modified Regulations, but have some constructive feedback around certain provisions within the proposed language.

IA COMMENTS

General

As we noted in our comments to the Third Set of Proposed Modifications to CCPA Regulations, IA member companies are concerned about the continuous nature of the CCPA regulations process. We appreciate the AGO doing its part to protect consumers and clarify or provide guidance for some of the confusing language within the CCPA. However, adding new requirements—as these modifications do—makes compliance more difficult for businesses and negatively impacts consumers’ abilities to exercise their rights under the law. While we are supportive of the AGO’s goal to provide greater clarity, closing the door on the rulemaking process for a period of time will allow businesses to implement the current regulations and regulators to identify the true challenges within the new rules.

W400-1

999.306 (f)

There are several issues with the proposed modifications for an opt-out button and IA respectfully requests that subsection (f) be removed from the proposed modified regulations for the following reasons.

W400-2,
W400-3,
W400-4,
and
W400-5

¹ IA’s full list of members is available at: <https://internetassociation.org/our-members/>.

² IA Privacy Principles for a Modern National Regulatory Framework, available at: https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_fulldoc/ (last accessed November 25, 2019).



● Section 999.306 (f) (1-2)

- **The interplay between proposed (f)(1) and (f)(2) language is difficult to interpret for both businesses and will ultimately negatively impact consumers.** First, (f)(1) states that the opt-out button may be used in *addition* to posting the notice of right to opt-out, but not “in lieu of” the requirements to post the notice of right to opt-out or the “Do Not Sell My Personal Information” link. Alternatively, subsection (f)(2) seems to require the opt-out button to be added to the left of the “Do Not Sell My Personal Information” link where a business posts it, thus implying that the button is not in fact an optional addition, but instead a requirement.

These conflicting subsections create confusion for both consumers and businesses alike. Businesses looking to comply with the CCPA will suffer from not having a clear standard for implementing their tools to allow consumers to opt out. Consumers will also not be able to identify if they have truly opted out of their personal information being sold with so many different options and links between a “Do Not Sell My Personal Information” button, an opt out toggle, and the language contained in the privacy policy. IA supports the AGO’s goals to have clear and easy to use functions when it comes to consumers actively controlling their personal data, but these provisions do not allow for a consistent and workable standard. Therefore, IA recommends either (1) providing further explanation and clarity to these subsections or (2) removing these proposed modifications to the CCPA.

W400-2

- **Subsection (f)(2)’s location requirement for the opt out button does not take into account the various mediums of the internet ecosystem.** The provision requires the button next to the “Do Not Sell My Personal Information” link and that it must link to the same notice of right to opt out page as the “Do Not Sell My Personal Information” link. The potential value this button may provide is outweighed by the fact that websites often have limited space, which is especially true for mobile-optimized sites and within mobile apps. In certain circumstances it may be impossible to add this image next to the “Do Not Sell My Personal Information” link in the app’s Settings page, or on the app’s download page of the app store.

W400-3

- **The proposed opt-out button design is impractical for businesses and consumers.** The proposed button image with a check mark and an “X” mark next to each other is confusing for consumers. It is not easy to identify which mark indicates a consumer has opted out of the sale of their personal data or whether the consumer has taken any action based on the toggle design. Further, the toggle design is not a choice for opting in or opting out for the consumer, but instead a repetitive link for the same place as the “Do Not Sell My Personal Information” button. IA believes this button should be modified in some way from its current design due to (1) the unclear intent of the design and (2) the redundancy of the button, which could cause confusion for consumers wishing to opt out of the sale of their information.

W400-4

● Section 999.306 (f)(3)

- Finally, the requirement in (f)(3) that the opt-out button be “the same size as any other buttons” is similarly confusing. Button sizes are often inconsistent across different pages and between websites, mobile-optimized pages, and mobile apps. It’s unclear whether the button should be the same size as other buttons on that particular page or across multiple pages of a website. This requirement is difficult for businesses to interpret and is likely to result in

W400-5



inconsistent compliance at best and an impossible standard at worst.

W400-5
cont

999.315 (h)

• Section 999.315 (h)(1-5)

- These sections are intended to provide illustrative examples of how businesses should make requests to opt-out easy for consumers to execute. While the examples are intended to provide clarity, they are framed in a statutory “shall not” form, implying that businesses must comply with their prescriptions.
- IA would recommend the following suggestions below that are inspired by the six verification considerations set forth in section 999.323 (b)(3). Under the aforementioned section, the regulations present the format of a consideration and how a business should apply that consideration. Using this format provides businesses with greater clarity and guidance about how to design and process consumer requests to opt-out.

• (h)(3)

- IA member companies are concerned about the current language of (h)(3) limiting businesses’ ability to provide more transparency to consumers. As currently drafted, this subsection could potentially inhibit companies from providing additional context and information to consumers about how they protect and use consumer data. We would recommend that the AGO review this language and IA’s recommendations below to provide consumers with the ability to fully understand the implications of choosing to opt-out prior to making their decision.
- Furthermore, IA is concerned that (h)(3) may raise compelled speech issues, as it would prohibit companies from providing consumers with additional information about the implications of their opt-out.
- IA member companies would encourage the AGO to consider adopting a reasonableness standard, as noted below, for what information companies can provide to consumers during the opt-out decision process. Our companies would like to supply pertinent and reasonable information to consumers to help them make informed decisions about the use of their personal information.

○ IA Suggested Text Alterations:

- (h) A business’s methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose ~~or has the substantial effect~~ of subverting or impairing a consumer’s choice to opt-out. A business shall consider the following factors when creating processes for requests to opt-out: ~~Illustrative examples follow:~~
 - (1) The number of steps included in the business’s process for submitting a request to opt-out as compared to the number of steps included in the ~~shall not require more steps than that~~ business’s process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a

W400-6



request to opt-out ~~should be~~ measured from when the consumer clicks on the “Do Not Sell My Personal Information” link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information ~~should be~~ measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request. The number of steps included in the business’s process for submitting a request to opt-out should not unreasonably exceed the number of steps included in the business’s process for a consumer to opt-in to the sale of personal information after having previously opted out.

- (2) ~~Whether the business uses~~ ~~A business shall not use~~ confusing language, such as double-negatives (e.g., “Don’t Not Sell My Personal Information”), when providing consumers the choice to opt-out. The business should avoid using confusing language such as double-negatives.
- (3) ~~Whether a business unreasonably requires~~ ~~Except as permitted by these regulations, a business shall not require~~ consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request. The business should avoid unreasonably requiring consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request, except as permitted by these regulations.
- (4) ~~Whether t~~The business’s process for submitting a request to opt-out ~~shall not requires~~ the consumer to provide personal information that is not necessary to implement the request. The business should avoid requiring consumers to provide personal information that is not necessary to implement the request to opt-out.
- (5) ~~Whether, u~~Upon clicking the “Do Not Sell My Personal Information” link, the business ~~shall not requires~~ the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out. The business should avoid requiring consumers to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.

W400-6
cont

Respectfully,

Dylan Hoffman
Director of California Government Affairs
Internet Association

From: [Monticollo, Allaire](#)
To: [Privacy Regulations](#)
Cc: [Signorelli, Michael A.](#)
Subject: Joint Ad Trade Comments on Fourth Set of Proposed Modifications to Text of CCPA Regulations
Date: Sunday, December 27, 2020 11:05:12 AM
Attachments: [FINAL Joint Ad Trade Comments on Fourth Set of Modifications to CCPA Regulations.pdf](#)

Dear Privacy Regulations Coordinator:

Please find attached joint comments from the following advertising trade associations on the content of the fourth set of proposed modifications to the text of the California Consumer Privacy Act regulations: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, the Digital Advertising Alliance, and the Network Advertising Initiative.

If you have any questions about these comments, please feel free to reach out to Mike Signorelli at [REDACTED]

Best Regards,
Allie Monticollo

Allaire Monticollo, Esq. | Venable LLP
t [REDACTED] | f 202.344.8300
600 Massachusetts Avenue, NW, Washington, DC 20001
[REDACTED] | www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



December 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Fourth Set of Proposed Modifications to Text of California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General (“OAG”) on the fourth set of proposed modifications to the text of the California Consumer Privacy Act (“CCPA”) regulations.¹

The undersigned organizations’ combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation’s digital advertising expenditures. Locally, our members are estimated to help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.²

For more than a year, our members have been communicating with consumers about their CCPA rights and how to effectuate them. As a result, our members have experience in operating under the CCPA and interacting with consumers. We have learned valuable insights about how to support consumer privacy rights under this new legal regime, including that operational flexibility is vital.

Not all interactions with consumers are the same nor are all business operations. There is no “one-size fits all” approach to the CCPA. We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous comment submissions and in this letter, the draft regulations implementing the CCPA should be updated to provide greater clarity, better enable consumers to exercise informed choices, and help businesses in their efforts to continue to provide value to Californians and support the state’s economy.³

See Below

¹ See California Department of Justice, *Notice of Fourth Set of Proposed Modifications to Text of Regulations and Addition of Documents and Information to Rulemaking File* (Dec. 10, 2020), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-4th-set-mods.pdf>.

² IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at http://www.ana_net/getfile/23045.

³ Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG’s proposed rules implementing the CCPA. See *Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set1.pdf> at CCPA_15DAY_000554 - 000559; *Second Set of Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA_2ND15DAY_00309 - 00313; *Third Set of Proposed Regulations Implementing the California Consumer*

Companies and consumers have been adapting to the “Do Not Sell My Personal Information” tagline for more than a year. This effort has included refashioning digital properties, as well as instituting backend processes to meet the compliance requirements of the CCPA even as a new ballot initiative, the California Privacy Rights Act (or “Proposition 24”), was moving forward. These most recent proposed modifications by the OAG to the CCPA regulations set forth ambiguous terms surrounding a proposed online button almost a full year after the law went into effect. Among other things, this round of modifications fails to clarify whether the button is optional or mandatory. The proposed changes also do not leave room for the deployment of alternative icons, such as the CCPA Privacy Rights Icon in market provided by the Digital Advertising Alliance (“DAA”),⁴ or other methods, such as a text only link in applicable scenarios, to facilitate consumers’ right to opt out of personal information sales. The OAG should reconsider these provisions, or at the very least clarify them so businesses can take steps to comply with the new terms as soon as possible.

See Below
cont

Additionally, changes the OAG made during the third set of proposed modifications to the CCPA regulations set forth a prescriptive interpretation of the law that could limit businesses’ ability to support employment in California and the state’s economy during these unprecedented times. We reassert the issues we previously raised with those provisions in this submission. As explained in more detail in the sections that follow below, the OAG’s potential changes to Section 999.315 would inhibit consumers from receiving transparent information and impinge on businesses’ right to free speech. In addition, the proposed modifications to Section 999.326 would not provide any protections for consumers related to their communications with authorized agents, as such agents are not presently held to similar consumer notice rules as businesses. Finally, the OAG’s proposed edits to Section 999.306 regarding offline notice of the right to opt out could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify these changes per the below comments.

Our members are committed to offering consumers robust privacy protections while simultaneously providing them with access to ad-funded news, apps, and a host of additional online services. These are offerings we have all become much more dependent on in recent months with the widespread proliferation of the COVID-19 pandemic. Ad-supported online content and services have been available to consumers and will continue to be available to consumers so long as laws allow for innovation and flexibility without unnecessarily tilting the playing field away from the ad-subsidized model. We believe a regulatory scheme that offers strong individual privacy protections and enables continued economic advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA regulations for Californians as well as protect the economy.

I. The Regulations Should Clarify That the Proposed New Button is Discretionary and Not Preclude Use of Other Icons Presented in Conjunction with the Text Link

In the fourth set of proposed modifications to the CCPA regulations, the OAG reinserted terms setting forth a specific graphic for a button enabling consumers to opt out of personal information sales. The proposed modifications state that the proposed button “*may* be used” in addition to posting a notice of the right to opt-out online, but not in lieu of such notice or the “Do Not Sell My Personal Information” link.⁵ In the very next subsection, the proposed rules state that when a business provides a “Do Not Sell My Personal Information” link, the proposed button “*shall* be added to the left” of the link.⁶ The language describing the proposed button is thus unclear, as it does not adequately explain whether providing the

W401-1

Privacy Act, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf> at CCPA_3RD15DAY_00111 - 00118.

⁴ DAA, *Opt Out Tools*, located at <https://www.privacyrights.info/>.

⁵ Cal. Code Regs. tit. 11, § 999.306(f)(1) (proposed Dec. 10, 2020) (emphasis added).

⁶ *Id.* at § 999.306(f)(2) (emphasis added).

button is discretionary or mandatory for businesses that sell personal information. We ask the OAG to confirm that the proposed button is discretionary as well as to provide flexibility for businesses to use alternative, industry-developed icons that signal the right to opt out of personal information sales to California consumers.

W401-1
cont

As the founding members of the DAA YourAdChoices program and corresponding icon,⁷ we understand the benefits a widely recognizable icon can bring to provide transparency and choices to consumers. In fact, in November 2019, the DAA announced its creation of a tool and corresponding Privacy Rights Icon to provide consumers with a clear and recognizable mechanism to opt out of personal information sales under the CCPA.⁸ Icons and corresponding privacy programs created by the DAA have a history of success. The YourAdChoices icon has been served globally at a rate of more than one trillion times per month, and its recognition continues to grow. In a 2016 survey, more than three in five respondents (61 percent) recognized the YourAdChoices icon at least a little, and half (50 percent) said they recognized it a lot or somewhat. For the CCPA, there is a need for flexibility in how this novel law is implemented in the market. The OAG should allow the marketplace to determine the best opt-out button approach, including allowing the option for use of an icon promulgated in relation to industry-driven opt-out mechanisms, rather than creating uncertainty by mandating a new graphic that businesses must use.

W401-2

Moreover, adding the button as a requirement now, nearly a year after the CCPA became effective and more than five months after the OAG began enforcing the law, would create unnecessary new compliance costs for businesses to reconfigure websites and consumer-facing properties after they have already taken significant steps to update their practices per the CCPA's requirements. We therefore ask the OAG to clarify that the new opt-out button is discretionary rather than mandatory, and businesses that provide a "Do Not Sell My Personal Information" link are not required to also provide the proposed button. We also ask the OAG to provide flexibility for businesses to utilize other icons to signal a consumer's right to opt out of personal information sales, such as the DAA's CCPA Privacy Rights Icon. The OAG should reconsider the need to create new iconography and should instead partner with industry on the already existing DAA Privacy Rights Icon to help lead consumers to choices about how their personal information is used and shared.

W401-3

See Above

II. The Regulations Should Support Consumers' Awareness of the Implications of Their Privacy Decisions, Not Hinder It in Violation of the First Amendment

The proposed online and offline modifications unreasonably limit consumers' ability to access accurate and informative disclosures about business practices as they engage in the opt out process. Ultimately, this restriction on speech would not benefit consumers or advance a substantial interest. The proposed rules state: "Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request."⁹ This language unduly limits consumers from receiving important information as they submit opt out requests. It is also overly limiting in the way that businesses may communicate with consumers. As highlighted above, data-driven advertising provides consumers with immensely valuable digital content for free or low-cost, as well as critical revenue for publishers, by increasing the value of ads served to consumers. As the research cited above also confirms, consumers have continually expressed their preference for ad-supported digital content and services, rather than having to pay significant fees for a wide range of apps, websites, and internet services they use. However, as a result of the proposed modifications, consumers' receipt of factual, critical information about the nature of the ad-supported

W401-4

⁷ Digital Advertising Alliance, *YourAdChoices*, located at <https://youradchoices.com/>.

⁸ DAA, *Digital Advertising Alliance Announces CCPA Tools for Ad Industry* (Nov. 25, 2019), located at <https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-announces-ccpa-tools-ad-industry>.

⁹ Cal. Code Regs. tit 11, § 999.315(h)(3) (proposed Oct. 12, 2020).

Internet would be unduly hindered, thereby undermining a consumer’s ability to make an informed decision. A business should be able to effectively communicate with consumers to inform them about how and why their data is used, and the benefit that data-driven advertising provides as a critical source of revenue.

It is no secret that consumers greatly value the information they can freely access online from digital publishers. However, local news publishers, for instance, continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising.¹⁰ However, the proposed modifications, as drafted, could obstruct consumers from receiving truthful, important information by hindering a business’ provision of a reasonable notice to consumers about the funding challenges opt outs pose to their business model.

The CCPA regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt out process. The proposed modification would impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet, and, as explained in Section III, they may be contemporaneously receiving partial or misleading negative information about their opt out rights.

To ensure a fully informed privacy choice, consumers must have every ability to access information about business practices and the benefits of the digital advertising ecosystem. Providing ample and timely opportunities for consumers to gain knowledge about their choice to opt out is of paramount importance to avoid confusion and ignorance; this allows a consumer to be fully informed about the actual implications of their decision. By prohibiting a business from requiring a consumer “to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request” the regulations do not safeguard against this concern. As presently written, the proposed modification appears to limit businesses’ ability to provide such vital information as a consumer is opting out, even if such information is presented in a seamless way. It is unclear what amount of information, or what method in which such information is presented, could constitute a violation of the rules. Instead of setting forth prohibitive rules that could reduce the amount of information and transparency available to consumers online, the OAG should prioritize facilitating accurate and educational exchanges of information from businesses to consumers. As a result, we ask the OAG to revise the text of the proposed modification in Section 999.315(h)(3) so that businesses are permitted to describe the impacts of an opt-out choice while facilitating the consumer’s request to opt out.

Additionally, the restrictions created by this proposed modification infringe on businesses’ First and Fourteenth Amendment right to commercial speech. As written, Section 999.315(h)(3) restricts the information consumers can receive from businesses as they submit opt out requests by limiting the provision of accurate and truthful information to consumers. The Supreme Court has explained that “people will perceive their own best interest if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . .”¹¹ Because this proposed regulation prescriptively regulates channels of communication, it violates the First and Fourteenth Amendments.

The state may not suppress speech that is “neither misleading nor related to unlawful activity” unless it has a substantial interest in restricting this speech, the regulation directly advances that interest,

¹⁰ DAA, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located at <https://digitaladvertisingalliance.org/press-release/study-online-ad-value-spikes-when-data-used-boost-relevance>.

¹¹ *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U. S. 748, 770 (1976).

W401-4
cont

and the regulation is narrowly tailored to serve that interest.¹² The proposed regulation fails each part of the test:

- **No substantial interest:** Although there is no stated justification in the proposal, the most likely interest would be to streamline opt out requests by making it easier and faster to submit opt-outs. The OAG presumably wants nothing to impede consumers from opting out, but it is unclear because the OAG has not affirmatively stated its purpose for the proposed modification. Consumers should be made aware of the ramifications of their opt out decisions as they are opting out – not after confirming a request – so they do not make opt out choices to their detriment because they do not know the effect of such choices. For this reason, they should be able to receive information from businesses about the consequences of their opt out choices as they are submitting opt out requests. Providing information concerning the impact of an opt out is not an impediment to the process, but rather improves it.
- **No advancement of the interest:** If streamlining opt out requests to remove perceived impediments is the justification for the proposed rule, then the proposal does not advance that interest. The proposed regulation already includes many other specific requirements that facilitate speed and ease of opt-outs, including a requirement to use the minimal number of steps for opt-outs (and no more than the number of steps needed to opt in), prohibiting confusing wording, restricting the information collected, and prohibiting hiding the opt-out in a longer policy, all of which directly advance this interest without suppressing speech. The proposed rule limiting businesses from clicking through or listening to reasons would not make the opt out process easier for consumers, because it could result in consumers making uninformed choices if they are not notified of the consequences of their decision to opt out as they are making it. A “regulation may not be sustained if it provides only ineffective or remote support for the government’s purpose.”¹³ This proposed regulation is both ineffective and provides no support for the government’s purpose.
- **Not narrowly tailored:** The proposed regulation is an overly broad and prescriptive restriction on speech that hinders accurate and educational communications to consumers about the consequences of a decision to opt-out. The regulations already include various other provisions that work to streamline the opt out process. “[I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.”¹⁴ As noted above, there are many ways to craft regulations to require simple and fast opt-out mechanisms that do not suppress lawful and truthful speech.

In sum, the regulation violates each and every prong of the framework for evaluating commercial speech. “As in other contexts, these standards ensure not only that the state’s interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message.”¹⁵ The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The U.S. Supreme Court has made clear that the burden is on the government to justify content-based restrictions on lawful speech, and the failure to even state a basis for this restriction fails to meet this requirement.¹⁶ The OAG should revise the text of the proposed

¹² *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980); see also *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

¹³ *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).

¹⁴ *Id.*

¹⁵ *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).

¹⁶ *E.g., Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (citing *Arizona Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721 (2011)).

modification in Section 999.315(h)(3) to avoid running afoul of the First and Fourteenth Amendments and to ensure consumers may receive information about the impacts of an opt out request as they engage in the opt out process with a business.

W401-4
cont

III. The Proposed Modifications Should Impose the Same Notice Requirements on Authorized Agents as They Impose on Businesses

The proposed modifications to the CCPA regulations would require a business to ask an authorized agent for proof that a consumer gave the agent signed permission to submit a rights request.¹⁷ Although this provision helps ensure businesses can take steps to verify that authorized agents are acting on the true expressed wishes of consumers, the proposed modifications do not offer consumers sufficient protections from potential deception by authorized agents. For example, while the proposed modifications would impose additional notice obligations on businesses,¹⁸ those requirements do not extend to authorized agents. Authorized agents consequently have little to no guidelines or rules they must follow with respect to their communications with consumers, while businesses are subject to onerous, highly restrictive requirements regarding the mode and content of the information they may provide to Californians. The asymmetry between the substantial disclosure obligations for businesses and the lack thereof for authorized agents could enable some agents to give consumers misleading or incomplete information. We encourage the OAG to take steps to modify the proposed modifications to the CCPA regulations in order to equalize the notice requirements placed on businesses and agents, thus ensuring consumers can act on an informed basis under CCPA. In Section II of this submission, we discuss related First Amendment and communications fairness issues implicit in a balanced consumer privacy notice regime.

W401-5

IV. Proposed Modifications to the CCPA Regulations Should Enable Flexibility in Methods of Providing Offline Notice

The proposed modifications to the CCPA regulations related to offline notices present a number of problems for consumers and businesses. As written, the CCPA implementing regulations already provide sufficient guidance to businesses regarding the provision of offline notice at the point of personal information collection in brick-and-mortar stores.¹⁹ The proposed modifications are more restrictive and prescriptive than the current plain text of the CCPA regulations, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. We therefore ask the OAG to update the proposed modifications to: (1) remove the proposed illustrative example associated with brick-and-mortar stores, and (2) explicitly enable businesses communicating with Californians by phone to direct them to an online notice where CCPA-required disclosures are made to satisfy their offline notice obligation, a medium which is more familiar to consumers for these sorts of disclosures along with having the added benefit of being able to present additional choices to the consumer. This sort of operational flexibility is necessary for businesses to convey important notices in context.

W401-6

The proposed modifications would require businesses that sell personal information to “inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request” when interacting with consumers offline.²⁰ The proposed modifications proceed to offer the following “illustrative examples” of ways businesses may provide such notice: through signage in an area where the personal information is collected or on the paper forms that collect personal information in a

¹⁷ Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).

¹⁸ *Id.* at § 999.315(h)(3).

¹⁹ Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).

²⁰ Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Dec. 10, 2020).

brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.²¹ While the illustrative examples set forth limited ways businesses can give notice in compliance with the CCPA, they are more restrictive than existing provisions of the CCPA regulations and detract from the flexibility businesses need to provide required notices that do not burden consumers or cause unreasonable friction or frustration during the consumer’s interaction with the business.

The illustrative example related to brick-and-mortar store notification sets forth redundant methods by which businesses may provide notices in offline contexts. The CCPA regulations already address such methods of providing offline notice at the point of personal information collection by stating, “[w]hen a business collects... personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.”²² The proposed modifications regarding notice of the right to opt out in offline contexts are therefore unnecessary, as the regulations already address the very same methods of providing offline notice and offer sufficient clarity and flexibility to businesses in providing such notice.

In addition, the proposed modifications related to brick-and-mortar store notification are overly prescriptive. They include specific requirements about the *proximity* of the offline notice to the area where personal information is collected in a store. The specificity of these illustrative examples could result in over-notification throughout a store as well as significant costs. For example, the proposed modification could be interpreted to require signage at each cash register in a grocery store, as well as signage at the customer service desk, in the bakery area of the store where consumers can submit requests for cake deliveries, and in any other location where personal information may be collected. They also do not account for different contexts of business interactions with consumers. A business operating a food truck, for instance, would have different offline notice capabilities than an apparel store. A single displayed sign in a brick-and-mortar store, or providing a paper version of notice, would in most instances provide sufficient notice to consumers of their right to opt out under the CCPA. Bombarding consumers with physical signs at every potential point of personal information collection could be overwhelming and would ultimately not provide consumers with more awareness of their privacy rights. In fact, this strategy is more likely to create privacy notice fatigue than any meaningful increase in privacy control, thus undercutting the very goals of the CCPA.

Additionally, the proposed modifications’ illustrative example of providing notice orally to consumers on the phone appears to suggest that reading the full notice aloud is the only way businesses can provide CCPA-compliant notices via telephone conversations. Reading such notice aloud to consumers would unreasonably burden the consumer’s ability to interact efficiently with a business customer service representative and would likely result in consumer annoyance and frustration. Requiring businesses to keep consumers on the phone for longer than needed to address the purpose for which the consumer contacted the business would introduce unneeded friction into business-consumer relations. Instead, businesses should be permitted to direct a consumer to an online link where information about the right to opt out is posted rather than provide an oral catalog of information associated with particular individual rights under the CCPA.

The proposed modifications’ addition of illustrative examples regarding methods of offline notice is unnecessary, redundant, inflexible, and likely highly costly for many businesses. These modifications would result in consumer confusion, leave businesses wondering if they may take other approaches to offline notices, and if so, how they may provide such notice within the strictures of the CCPA. We therefore ask the OAG to remove the proposed illustrative example associated with brick-and mortar stores

²¹ *Id.*

²² Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).

as well as clarify that businesses communicating with consumers via telephone may direct them to an online website containing the required opt out notice as an acceptable way of communicating the right to opt out.

W401-6
cont

* * *

Thank you for the opportunity to submit input on the content of the proposed modifications to the CCPA regulations. Please contact Mike Signorelli of Venable LLP at [REDACTED] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance

From: [Cameron Demetre](#)
To: [Privacy Regulations](#)
Subject: TechNet 4th round of comments for CCPA Regulations
Date: Sunday, December 27, 2020 11:49:27 AM
Attachments: [TechNet CCPA Regulation Letter 12.27.20.pdf](#)

Hello Lisa,

Please see TechNet's letter regarding the fourth round of CCPA regulation comments.

Kind regards,

Cameron Demetre
Executive Director | California & the Southwest
[TechNet](#) / The Voice of the Innovation Economy
(c) [REDACTED] | [REDACTED]
Twitter: @TechNetSouthwest





December 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Department of Justice
300 Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Dear Attorney General Becerra,

TechNet appreciates the opportunity to submit written comments regarding the fourth set of proposed modifications to the California Consumer Privacy Act (“CCPA”) regulations.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet’s diverse membership includes dynamic startups and the most iconic companies on the planet and represents three million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet member companies place a high priority on consumer privacy. We appreciate the aim of the CCPA to meaningfully enhance data privacy and some of the latest modifications in response to the previous iteration of comments specifically as it relates to § 999.306, which will provide more clarity for consumers to help avoid confusion in offline settings and more acutely syncing with CCPA statute. However, we continue to be concerned that CCPA regulations are not finalized and it is not clear when these new draft regulations would be final and implemented. This raises significant compliance problems for a law that took effect January 1, 2020 and for which enforcement began July 1, 2020. We believe these modifications should include language making the changes effective six months to one year from publication of final regulations. This will give businesses the opportunity to properly implement complex regulations for a complex law. This implementation time is especially important during the ongoing COVID-19 crisis where personnel are working remotely and businesses are continuing to recover from services being shut down.

W402-1

W402-2

TechNet’s comments are concentrated on two components of the regulations:

1. § 999.326 Verification Requests of Authorized Agents

TechNet remains concerned as it relates to the role businesses should have in requiring identify verification for authorized agents — two forms of identify verification are necessary in helping to mitigate fraudulent activity. We believe a

W402-3

business should be allowed, both, to verify a consumer's identify and to also confirm that the consumer they provided the authorized agent permission to submit the request is valid in order to avoid identify theft.

W402-3
cont

2. § 999.306 Proposed Opt-Out Icon

The recent passage of Proposition 24- the California Privacy Rights Act (CPRA) requires a rulemaking which will establish a process to select an effective icon. This requisite renders a robust stakeholder process to identify the merits of any particular icon and the efficacy by which it will develop a concise, usable instrument. Identifying an icon now would circumvent the process just after one was approved by the voters. The icon development process should go through the CPRA route in the soon-to-be established California Privacy Protection Agency.

W402-4

Additionally, there remains a lack of clarity as to the discretion of utilizing the opt-out button identified in § 999.306. § 999.306 (f)(1) suggests companies have a choice with respect to whether they want to present the button, however, Section (f)(2) strongly suggests that the button is required for anyone putting up a Do Not Sell My Personal Information link. As a result, these provisions appear to conflict as to the requirement to include an Opt-Out icon. Withal, the requirement of the specific icon delineated in the regulations looks like a button adjacent to the link, which will only be confusing to consumers as it could be mistaken for a button to effectuate the opt-out, leading them to overlook the link itself. For these reasons, we believe the CPRA process will help to address some of these concerns.

W402-5

W402-6

TechNet thanks you for taking the time to consider our comments on the proposed modifications to the CCPA regulations. We again urge that any new proposed modifications give businesses proper time to come into compliance with the regulations. Our goal for all CCPA regulations is that they should help facilitate compliance on the part of California businesses, while ensuring that consumers have the information necessary for them to make informed decisions regarding their rights under the CCPA.

If you have any questions regarding this comment letter, please contact Cameron Demetre, Executive Director, at [REDACTED] or [REDACTED].

Thank you,



Cameron Demetre
Executive Director, California and the Southwest
TechNet

Privacy Regulations

From: Stephanie Lucas [REDACTED]
Sent: Sunday, December 27, 2020 3:07 PM
To: Privacy Regulations
Subject: Comment on 4th Set of Proposed Modifications: CCPA
Categories: Written Comment

My name is Stephanie Lucas, and I'm a web design professional (and a proud native Californian).

This is the first time I've used the public comment option on any legislation. First, I want to express that I understand how much work and effort your office has put into this process, and I appreciate the opportunity to comment.

I would like to respectfully voice specific technical considerations from the standpoint of web and app design. I have worked in the design field for over 25 years, and specifically in web and app design for about 15 years. Upon reviewing the guidance for the "button" as well as the research study that led to this design, I have significant concerns about this guidance, which I'll explain as concisely as I can.

First, here is the visual graphical element I'm referring to (for the remainder of this email I'm going to call it a "visual graphic element" because the taxonomy that's being used ("button"/"icon") is itself one of my principal concerns.



Next, to quote the "NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE":

"The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers."

My assertion is that this visual graphic element conflicts with this requirement in at least two ways, listed below.

Concern 1: Button, toggle, or Icon?

I'll have to beg your patience with this, but it's a legitimate issue. In the [study that informed this guidance](#), the visual graphic element is referred to throughout not as a "button" but as an "icon." This may seem like a silly distinction, but it isn't: **To be honest, this is actually a huge issue that questions the validity of applying this study to the Attorney General's guidance at all.**

W403-1

A **button** is the name of a design element that has a specific function *and specific rules and best practices*. A button needs to - on its own - *clearly represent what action it represents*. This is a very

foundational web design principle. Most buttons have text that states the action. This visual element has two abstract symbols that don't mean anything without context.

W403-1
cont

Buttons also have their own rules when it comes to programming for accessibility.

Further, it's evident that this new visual graphic element is an **iteration of the "red toggle"** from the initial guidance. I maintain it still will be mistaken for a toggle, or that at minimum there will be confusion caused by the visual similarity. A quick visual scan reveals 2 very toggle-type characteristics/cues: *1. It's basically the same shape as a toggle* *2. It's half/half blue and white, like a toggle.* Those characteristics should be reconsidered.

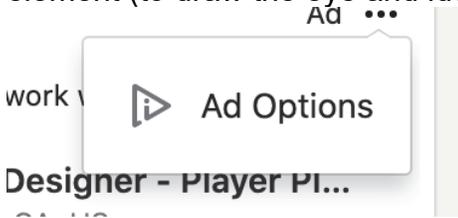
W403-2

By comparison, an **icon** is a visual symbol for *wayfinding and identifying*. Speaking from years of experience in this field: It's critically important to not conflate these two terms. Based on the purpose expressed in both the Attorney General's guidance and the study I linked, the element is meant to *draw the eye and make sense to the user to help them understand they have a choice*. That has the characteristics of an icon, not a button.

I'm not splitting hairs here: designers (the people who will have the job of implementation) will have a difficult time if there's ambiguity over whether this is a button or icon.

For example, the "Ad Options" visual element (the triangle) is an icon, not a button. I believe this icon is for the same purpose that the Attorney General's office has in mind for the CCPA visual graphic element (to draw the eye and identify).

W403-1
cont



Since the guidances have begun rolling out, I'm seeing both the term "button" and "icon" being used interchangeably in discussions - if you look ahead to the actual implementation phase of this, it's critical for product teams to understand whether it's an icon or a button. I believe the AG's office is going to create more confusion than solve it if this current guidance is delivered.

Concern 2: Accessibility

Again quoting "*NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE*" *the user experience should be:*

"reasonably accessible to consumers with disabilities"

W403-3

I am troubled to see that [the study that informed this decision the study that informed this decision](#) doesn't seem to have sought out any participants with disabilities (if it did, that doesn't seem to be communicated in the summary report).

It's important to understand that accessibility is ***not just making sure that elements work with screen reader technology***. Disability also extends to a spectrum of cognitive limitations as well as other considerations.

The CDC currently reports that over 25% of the population of California is contending with some type of disability.

If disabled individuals were not included in the study that examined comprehension and clarity around this visual graphic element, that means that *an enormous amount of consumers WON'T be served* by this requirement.

Since this new guidance was introduced in October, even so-called “abled” people - people with law degrees - have expressed confusion over what this visual graphic element means. What chance do consumers on the disability spectrum have?

Because the guidance appears to mandate the use of this visual graphic element, I think it's extremely important to get it right.

To summarize, in my opinion if this element is meant to draw the eye, it should:

- Be presented for user testing to study participants with a spectrum of disabilities
- Be re-evaluated to make it look less like a toggle
- Be consistently referred to as an *icon* and not a button, with guidance that it can *only be used if it's associated with text for context*
- Be optional

Thank you for your time. I am happy to be contacted for any further conversation on this at:

[REDACTED]

Stephanie Lucas

W403-3
cont

W403-2
cont

W403-1
cont

From: [Sara DePaul](#)
To: [Privacy Regulations](#)
Cc: [Carl Schonander](#); [Jeff Joseph](#); [Christopher Mohr](#); [Sara Kloek](#)
Subject: SIIA Comments to Notice of Fourth Set of Proposed Modifications to the CCPA Regulations
Date: Monday, December 28, 2020 9:20:35 AM
Attachments: [SIIA Comments CCPA Regs Fourth Modifications FNL.pdf](#)

On behalf of the Software & Information Industry Association (SIIA), I am attaching our comments to the notice of a fourth set of proposed modifications for filing by the deadline today. Thank you, and happy holidays.

Best,

Sara DePaul

Associate General Counsel & Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
1090 Vermont Ave NW, Sixth Floor, Washington, DC 20005
[REDACTED] Office / [REDACTED] Mobile / @saracdepaul Twitter
[sia.net/policy](#)



Accelerating Innovation in
Technology, Data & Media

202.289.7442
www.siiia.net

1090 Vermont Ave NW Sixth Floor
Washington DC 20005-4905

Software & Information Industry Association Comments Regarding the Notice of Fourth Set of Proposed Modifications to CCPA Regulation

The Software & Information Industry Association (SIIA) welcomes the opportunity to provide written comments regarding the Notice of Fourth Set of Proposed Modifications to the regulations regarding the California Consumer Privacy Act (CCPA). SIIA is the leading organization representing financial information, education technology, specialized content, information and publishing, and health technology companies. Our diverse membership of more than 700 companies and associations help learners of all ages prepare to succeed in their future, manage the global financial markets, develop software that solves today’s challenges, provide critical information that helps inform global businesses large and small, and innovate for better health care and personal wellness outcomes.

SIIA’s members are dedicated to data privacy, as a matter of regulatory obligation, responsible stewardship of data, and good customer care and service. On behalf of our members, we advocate for a national data privacy standard that robustly protects consumers while allowing innovation and competition. As you know, achieving these aims is complex and requires both thoughtful analysis of the impact of data provision regulatory provisions and identifying opportunities for interoperability with other data privacy frameworks when possible.

In general, we are neutral on the proposed modifications to the regulation. For the most part, the proposed modifications succeed in their goal to clarify existing regulatory provisions. We are concerned, however, by the proposed change to re-introduce an opt-button, albeit as a button that businesses that can optionally include next to their Do Not Sell link. While this is superficially consumer friendly, it is likely to lead to consumer confusion due to the lack of uniformity of use. Earlier provisions that would have mandated an opt-out button were removed for good reasons which likely will inhibit its adoption by businesses. We request that the Attorney General delete this proposed addition to Section 999.306, particularly at this late stage.

W404-1

Additionally, we are concerned with significant divergences between the CCPA, its implementing regulations, and the recently passed California Consumer Privacy Rights Act. We encourage the Attorney General to either use the CCPA rulemaking authority to close these gaps or to exercise his prosecutorial discretion to put industry on notice that they are not liable for business practices that will be lawful when the CPRA implements in 2023. We note two glaring gaps that require such action by the Attorney General.

W404-2

First, we remain concerned with the CCPA’s broad First Amendment defects, including with respect to its regulation of publicly available information. We have explained the substantive reasons for the CCPA’s First Amendment problems,¹ and will not repeat them here

¹ See SIIA’s March 27, 2020 Comments, available at: <https://www.siiia.net/Portals/0/pdf/Policy/Privacy%20and%20Data%20Security/SIIA%20Comments%20on%20CCPA%20Regs%2027%20MAR.pdf?ver=2020-03-30-092111-393>; February 25, 2020 Comments; available at: <https://www.siiia.net/Portals/0/pdf/Policy/SIIA%20Comments%20re%20CCPA%20Regs%20Feb%202020%20FNL%20FLD.pdf?ver=2020-03-27-131710-980>; December 6, 2019 Comments, available at:



in any depth, except to say that our prior filings have discussed the CCPA's unconstitutional regulation of public domain information that is widely available in private hands. And as we have brought to your attention in those same comments, your office is empowered by the CCPA to fix the statute's constitutional flaws through the rulemaking process. See *also* CCPA 1798.185(a)(3). Exercise of that power is imperative, not only with respect to insulating the CCPA from a fatal First Amendment attack but also to harmonize with the California Privacy Rights Act, which is constitutionally sound with respect to publicly available information.

The failure of the Attorney General's office to address this will create a significant practical problem. The CPRA will cure the CCPA's constitutionally invalid regulation of the public domain when it takes effect on January 1, 2023. Maintaining the CCPA's unconstitutional regulation in the intervening period, therefore, is neither beneficial to consumers nor businesses. For consumers, maintaining this unconstitutional reach extends "data rights" they are not entitled to as a matter of constitutional law and that will sunset by 2023. Business are presented with a Hobson's choice: they must either risk an enforcement action between now and the statute of limitations for the expiration of CCPA claims **or** bear the expensive burden of being whipsawed by a statutory obligation that will cease to exist in two years. Maintaining the CCPA's treatment of publicly available information will have consequences that are unfair, untenable, and unconstitutional.

We therefore respectfully urge the Attorney General to use his authority under Section 1798.185(a)(3) to standardize the treatment of publicly available information by either modifying the regulations to exclude the entire public domain as required by the First Amendment or to set forth an enforcement moratorium with respect to publicly available information that will be subject to the CPRA exclusions on January 1, 2023.

Second, the CCPA and CPRA's differences with respect to requests to opt-out and user-enabled global privacy controls create unfair and unnecessary compliance tensions. The implementing regulation for the CCPA, for instance, requires a business that collects personal information online to treat user-enabled global privacy controls as a signal of a consumer's choice to opt-out of the sale of their information. See Section 999.315(d). The CPRA, in contrast, does not require businesses to treat user-enabled global privacy controls as an opt-out. Instead, businesses can meet obligations relating to requests to opt-out either through the primary opt-out mechanism in Section 1798.135(a) *or* through an opt-out preference signal as set forth in Section 1798.135(b)(1). See *also* Section 1798.145(b)(3) ("A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).").

Barring action by the Attorney General to correct this discrepancy, businesses will be required either to risk enforcement action or comply with the CCPA by enabling both the Do Not

W404-2
cont

<https://www.siiia.net/Portals/0/pdf/Policy/SIIA%20Comments%20re%20CCPA%20regs%206%20DEC%20FNL%20%20FILED.pdf?ver=2020-01-17-135803-493>.



Sell Link **and** user-enabled privacy controls as requests to opt-out until January 1, 2023 when the CPRA implements and gives them a different choice. Leaving this conflicting obligation in place is unfair and against the wishes of the Californian electorate. As with the CCPA's unconstitutional regulation of the public domain, we urge the Attorney General to fix this tension either through the rulemaking process or through an enforcement policy statement that sets forth an intention not to bring enforcement actions for alleged CCPA violations that would not violate the CPRA.

W404-2
cont

Dated: December 28, 2020

Respectfully submitted,



Christopher A. Mohr, VP for Intellectual Property and General Counsel
Sara C. DePaul
Associate General Counsel & Senior Director for Technology Policy
Software & Information Industry Association
www.siiia.net

From: [Melanie Tiano](#)
To: [Privacy Regulations](#)
Subject: CTIA Comments Fourth Set of Modified Regulations
Date: Monday, December 28, 2020 12:31:13 PM
Attachments: [image002.png](#)
[CTIA - Comment on CCPA Fourth Set of Modified Regulations 12.28.20.pdf](#)

Good afternoon.

Attached are CTIA's comments in response to the Fourth Set of Modified Regulations.

Please let me know if you have any questions.

Thank you,

Melanie Tiano



Melanie K. Tiano
Director, Cybersecurity and Privacy
1400 16th Street, NW
Washington, DC 20036
[REDACTED] (office)
[REDACTED] (mobile)

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of)
)
California Consumer Privacy Act) Public Forums on the California
Rulemaking Process) Consumer Privacy Act
)
)

COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600 Washington,
DC 20036
(202) 736-3200
www.ctia.org

December 28, 2020

TABLE OF CONTENTS

INTRODUCTION 3

I. § 999.306 Notice of the Right to Opt-Out of the Sale of Personal Information 3

 a. The Department should clarify that use of an opt-out button is voluntary. 3

 b. The proposed button is potentially confusing to consumers..... 4

II. § 999.326. Authorized Agent..... 5

 a. CTIA requests that the Department maintain the current version of § 999.326 (a) but
 clarify that businesses may require authorized agents to verify their own identities. ... 5

CONCLUSION..... 7

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL’S OFFICE
Los Angeles, CA 90013

In the Matter of)
)
California Consumer Privacy Act Rulemaking) Public Forums on the California
Process) Consumer Privacy Act
)

INTRODUCTION

CTIA appreciates the opportunity to provide these comments on the California Department of Justice’s (“Department’s”) Fourth Set of Modified Proposed Regulations (“modified regulations”) to implement the California Consumer Protection Act of 2018 (“CCPA” or “Act”). CTIA appreciates the Department’s continued efforts to revise and clarify the final regulations. However, CTIA is concerned that regulations as the modifications propose may cause confusion, will not serve to further the purposes of the Act, and could allow for fraudulent requests for consumers’ personal information. CTIA’s concerns pertain to the following sections of the modified regulations:

- § 999.306. Notice of the Right to Opt-Out of the Sale of Personal Information; and
- § 999.326. Authorized Agent.

Where appropriate, CTIA provides alternative regulatory language to address the issues identified herein.

I. § 999.306 Notice of the Right to Opt-Out of the Sale of Personal Information

a. The Department should clarify that use of an opt-out button is voluntary.

CTIA appreciates the Department’s efforts to develop a framework for use of an opt-out button that is both consumer-friendly and practical. However, while it appears the intent of the

W405-1

Attorney General was to create a standardized, voluntary opt-out button,¹ the modified regulations create confusion due to inconsistencies between § 999.306(f)(1) and § 999.306(f)(2). In particular, subsection (1) states that the opt-out button “*may* be used in addition to posting the notice of the right to opt-out”, while subsection (2) states that the button “*shall* be added to the left of the [Do Not Sell My Personal Information Link].”

To avoid confusion and more clearly reflect the intent of the Attorney General, CTIA recommends that the Department revise § 306(f) as follows:

§ 999.306(f) . . . (1) *The following opt-out button may be used in addition to ~~posting the notice of right to opt-out~~, but not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations.*

(2) *Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button, ~~should the business choose to use it~~, shall be added to the left of the text as demonstrated below. The opt-out button, ~~if used~~, shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link.*

(3) *The button, ~~if used~~, shall be approximately the same size as any other buttons used by the business on its webpage.*

b. The proposed button is potentially confusing to consumers.

The design of the proposed opt-out button is potentially confusing and suffers from many of the same issues as the opt-out button proposed by the Department in its first set of modifications, dated February 10, 2020. CTIA has many of the same concerns with this button as it had with the initial opt-out button.²

¹ See Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, State of California Department of Justice, Office of the Attorney General (Oct. 11 2019) <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>, § 306 (e) (noting the process for development of a button that *may be used in addition to* but not in place of the posting of a notice of the right to opt out of the sale of personal information) (emphasis added).

² See Comments of CTIA, *In the Matter of California Consumer Privacy Act Regulations*, California Office of the Attorney General, Request for Comments, February 25, 2020 (noting that the proposed opt-out button was needlessly misleading because it gave the appearance of an immediate interactive opt-out control rather than a link to a page with more information).

W405-1
cont

W405-2

In particular, the presence of both a checkmark and an “x” may mislead consumers, who might reasonably believe that by: (1) clicking different sides of the button, consumers could indicate their distinct data selling preferences; (2) clicking the button, consumers could immediately operationalize their data selling preferences (as opposed to being directed to the same website as clicking on the adjacent “Do not sell my personal information” link); and/or (3) clicking the button, consumers could only indicate their consent to the sale of their personal information, which would otherwise be restricted. In addition, several participants in a study that originally tested the proposed opt-out button reported that they viewed the button as an opt-*in* mechanism.³

W405-2
cont

Accordingly, CTIA recommends that the Department reconsider the proposed design of the current proposed opt-out button, due to the risk it poses of confusing consumers.

II. § 999.326. Authorized Agent.

a. CTIA requests that the Department maintain the current version of § 999.326(a) but clarify that businesses may require authorized agents to verify their own identities.

CTIA reiterates the concerns expressed in its October 28, 2020 comment regarding the security risks associated with consumer information requests submitted through authorized agents.⁴ In particular, the revisions proposed to § 999.326(a) in the Third Set of Modified Proposed Regulations that remain in the current proposal would unnecessarily limit businesses’ ability to implement necessary antifraud measures related to verifying requests submitted by purported authorized agents. CTIA believes that the current version of § 999.326(a)⁵ provides a preferable framework for businesses to address such risks as compared to the revisions that

W405-3

³ Cranor et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* 31 (2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cranor-design-eval-usable-icon.pdf>.

⁴ See Comments of CTIA, *In the Matter of California Consumer Privacy Act Regulations*, California Office of the Attorney General, Request for Comments, October 28, 2020.

⁵ Cal Code Regs tit. 11, § 999.326(a) (2020).

remain in the current proposal. As noted in the Department’s Final Statement of Reasons, the current version of § 999.326(a) allows businesses the “discretion to determine, based on the [regulations’ general rules regarding identity verification],”⁶ which requirements set forth in § 999.326(a) are appropriate for a given request. In addition, the regulations’ general rules regarding identity verification contain guiding principles that require businesses to establish a “reasonable method” for verification, as well as “reasonable security measures to detect fraudulent identity-verification activity.”⁷

These guiding principles make clear that businesses’ identity verification processes, including for authorized agents, must be reasonable in light of the particular circumstances at issue. The limitations proposed in the modified regulations, on the other hand, would prohibit businesses from requiring all of the forms of verification outlined in § 999.326(a) *even if requiring all of those measures would be reasonable* in light of the security risks facing that particular business and its consumers.

In addition, and in accordance with these principles, CTIA recommends that businesses be expressly permitted to require authorized agents to verify their own identity. This additional verification measure may be necessary to avoid situations whereby fraudsters pose as authorized agents to gain access to consumers’ personal information, and businesses should have the flexibility to employ such a measure where appropriate.

CTIA therefore requests that the Department maintain the current version of § 999.326, and clarify that businesses may require authorized agents to verify their own identities, and proposes the following language be inserted into the current version of § 999.326(a):

⁶ Final Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, State of California Department of Justice, Office of the Attorney General 48 (June 1, 2020) <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf>.

⁷ Cal Code Regs tit. 11, § 999.323 (2020).

W405-3
cont

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the authorized agent verify their own identity and/or that the consumer do the following:

W405-3
cont

CONCLUSION

CTIA appreciates the Department's consideration of these comments and stands ready to provide any additional information that would be helpful.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA

1400 16th St. NW, Suite 600
Washington, DC 20036

(202) 736-3200

December 28, 2020

From: [Emery, Emily](#)
To: [Privacy Regulations](#)
Subject: MPA Comments on Fourth Set of Proposed Modifications to Text of CCPA Regulations
Date: Monday, December 28, 2020 1:09:57 PM
Attachments: [MPA Comments on Fourth Set of Proposed CCPA Modifications.pdf](#)

Attached, please find comments on the fourth set of proposed modifications to the text of regulations implementing CCPA submitted on behalf of MPA - The Association of Magazine Media.

We appreciate the opportunity to provide the attached comments for your consideration.

Wishing you a happy new year,
Emily Emery

Emily Emery
Director of Digital Policy
MPA - The Association of Magazine Media
Cell: [REDACTED]
Office: [REDACTED]
[REDACTED]

December 28, 2020

The Honorable Xavier Becerra
California Department of Justice
ATTN: Lisa B. Kim, Privacy Regulations Coordinator
300 South Spring Street, First Floor, Los Angeles, CA 90013

Submitted via email to PrivacyRegulations@doj.ca.gov

RE: Comments from MPA – the Association of Magazine Media on the Fourth Set of Proposed Modifications to Text of Regulations to Rulemaking [OAL File No. 2019-1001-05]

Dear Attorney General Becerra:

MPA – the Association of Magazine Media represents over 500 magazine media brands that deliver compelling and engaging content across online, mobile, video, and print media. Having testified on behalf of our members and provided previous rounds of comments on modified language proposed by the Office of the Attorney General (“OAG”), we appreciate the opportunity to offer additional comments on the fourth set of proposed modifications to the regulations implementing the California Consumer Privacy Act (“CCPA”).

On the date of these comments, the rulemaking provisions of the California Privacy Rights Act (“CPRA”) are already in effect. Further, the CCPA implementation process is now in its second year. Our members have devoted significant resources to make good-faith efforts to comply with existing CCPA requirements and will continue to invest in preparing for CPRA compliance. We ask that the OAG keep these efforts in mind when considering any additional proposed changes as businesses seek to simultaneously implement both the impending CPRA privacy framework and modifications to the current framework.

In response to the latest proposed modifications in the sections below, MPA offers the following recommendations concerning requirements for offline notice of right to opt-out, the proposed number of allowable steps for opt-out, and requests made through authorized agents. MPA’s suggested additions are indicated in ***bold italicized underline***.

I. The OAG should clarify in its modifications to Section 999.306(b)(3) that in instances where personal information is collected through a printed form that is to be mailed back to the company, that the offline notice may include a web address that the customer can access to opt-out of the sale of their personal information.

MPA appreciates the clarifying language proposed by the OAG on Section 999.306(b)(3) that makes the notification process for the right to opt-out more evident for businesses seeking to

W406-1

implement the requirement. In addition to collecting personal information online and at brick-and-mortar locations, the magazine media industry, as with other industries, may collect personal information that consumers complete through a printed form and then submit by mail, such as an order card inserted in a print issue of a magazine.

Magazine readers support and understand that publishers may use the information collected to offer other titles of interest, product recommendations, or in the furtherance of other positive consumer experiences. Publishers support making it easy for a consumer to understand how to opt-out of these offerings, including when a consumer submits information through a printed form that the consumer mails back to the business.

Where businesses like magazine publishers execute the common, expected, and CCPA-compliant practice of leveraging consumer data collected through offline means, the OAG should confirm that to provide notice at the point of collection of personal information, it is sufficient for a business to direct a customer to a web address where the consumer may choose to instruct the business that sells personal information to stop selling their personal information.

MPA made the following recommendation in [comments](#) regarding the third round of proposed modifications and raises it again here: MPA recommends that the OAG modify Section 999.306(b)(3) to include an additional illustrative example:

(c) A business that sells personal information from consumers that it collects through printed forms by mail may provide notice by including on the paper forms that collect the personal information a web address directing consumers to where the consumer may choose to opt-out of the sale of their personal information.

This addition – clarifying that providing a web address on printed material is an offline notice – would aid in compliance for offline printed notices. This illustrative example for printed materials sent through the mail is consistent with Section 999.305(b)(3) in which offline notices may direct consumers to where the “Do Not Sell My Personal Information” webpage can be found online. It is also analogous to the proposed illustrative example in Section 999.306(b)(3)(a) for brick-and-mortar stores (which may post signage).

This method of notice also enhances data privacy and security by minimizing the amount of data a business must collect in printed form to validate and execute a consumer’s request, allowing businesses to standardize operations, including the ability to have a single, centralized location where opt-out information is maintained.

II. The OAG should clarify in Section 999.315 that offers to customers are allowed if the display of such offers adds no additional steps to the opt-out process.

MPA agrees that the steps for submitting a request to opt-out should be minimal and should not subvert consumer intent. Magazine media consumers often benefit from renewal offers that reduce the price of a subscription. Posting notice of an offer of a discounted subscription without

W406-1
cont

W406-2

creating an additional required step or friction for the consumer provides value to the consumer without impairing a consumer's ability to execute their request to opt-out. The CCPA regulations should explicitly permit businesses to present a notice of benefits for the consumer should they elect to remain opted-in.

Consumers may also benefit from electing to opt-out of certain services or offerings while not opting-out entirely. Businesses should be permitted to enhance the consumer experience and better serve consumer intent by providing an easy opt-out process that allows the consumer to indicate his or her desired preferences. Businesses should be allowed to display an interface that enables the consumer to effectuate a full or partial opt-out or select/de-select from a listing where multiple offerings exist as long as one of the de-selection options is inclusive of all of the business' use of consumer data.

MPA made the following recommendation in [comments](#) regarding the third round of proposed modifications, and again in these comments: MPA urges the OAG to add the following clarification to Section 999.315(h)(3):

(3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request. *A business may display information that provides context to enable a consumer to reconsider their interest in opt-out or to elect a partial opt-out provided that display does not require additional steps or subvert or impair a consumer's choice to opt-out. A display that provides an offer of additional goods or services shall not count in the number of steps to opt-out if the consumer is not required to take an additional step if they do not wish to take advantage of the offer.*

III. In Section 999.326(a) on authorized agents, the OAG should restore businesses' ability to make good-faith efforts to engage with the consumer to both directly verify their identity and confirm with the consumer that they have authorized an agent's request.

MPA welcomes the additional clarifying text from the OAG that businesses may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request.

MPA urges the OAG to make an additional modification to the proposed text that would further improve businesses' ability to make good-faith efforts to protect consumers' data privacy and security.

The statutory CCPA text allows businesses to authenticate "right to know" and data deletion requests filed by consumers directly or through authorized agents and to do so by presenting the same interface online for either method. For example, businesses currently commonly utilize a consumer's email address to map to an account and process a request.

Since the effective date of the CCPA, many businesses have identified troubling practices by authorized agents that undermine consumers' data privacy and security, and these unauthorized

W406-2
cont

W406-3

requests continue to escalate. Therefore, MPA is concerned that in precluding businesses' ability to seek both verification and confirmation of authorization, the proposed language in Section 999.326(a) will impede necessary steps that businesses would take to respond to suspected consumer fraud instances perpetrated by entities improperly representing themselves as authorized agents.

Maximizing consumer data protection requires that businesses may both directly verify identity with the person to whom the request is related and confirm that the consumer provided the agent's authorization to submit the request. While MPA appreciates the addition of requiring a consumer to provide signed permission to the authorized agent, the most secure verification method remains in allowing a business to have direct contact with the consumer to both confirm identity and confirm that the consumer granted permission to an authorized agent.

If a business can only verify the consumer's identity, they're not able to alert the customer to a potentially unauthorized request. If a business can only confirm that an individual granted authorization, the unverified respondent of such an authorization request could still be the perpetrator of the unauthorized request. Both of these scenarios imperil consumers' data.

Requiring both steps is necessary for data security best practices, and businesses can execute both steps in a single correspondence to minimize inconvenience for the consumer.

W406-3
cont

MPA made the following recommendation in [comments](#) regarding the third round of proposed modifications, and again in these comments. MPA urges the OAG to restore the enacted text that allows businesses to exercise both verification methods:

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to ~~do either of the following~~:

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

MPA again notes the critical role that direct first-party engagement with consumers can have in enhancing data security, protecting privacy, and preventing fraudulent activity.

MPA and our members appreciate the opportunity to provide our views for your consideration.

In adopting the clarifications proposed above, the OAG will enhance the magazine media industry's ability to operationalize consistent privacy-protective practices that enhance reader trust, preserve the viability of media resources that consumers enjoy, and sustain vital journalism on which consumers rely for critical information.

Respectfully submitted,

Brigitte Schmidt Gwyn
President and Chief Executive Officer

Rita Cohen
Senior Vice President, Legislative and Regulatory Policy

Emily Emery
Director, Digital Policy

From: [Dale Smith](#)
To: [Privacy Regulations](#)
Cc: [Dale R. Smith Jr.](#)
Subject: Submission of Comments: NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS
Date: Monday, December 28, 2020 1:15:23 PM
Attachments: [footerNew2.bmp](#)
[20201228 CCPA Comments \(1\).pdf](#)

Dear Ms. Kim:

Attached please find our .pdf document containing comments relating to the 4th set of proposed CCPA regulation modifications.

Please contact me if you have any difficulty with their usage.

Thank you, and best wishes for a safe and happy 2021.

Dale Smith, CIPT

DALE R. SMITH, CIPT

Futurist | 



View my blog at: privacyelephant.com



December 28, 2020

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Via Email to: PrivacyRegulations@doj.ca.gov

Attn: Honorable Xavier Becerra, Attorney General

Re: Comments on NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS, Released December 10, 2020

Dear Mr. Becerra:

The subject of this comment is the newly-added “Opt-Out Button” proposed in §999.306(f) and the overall effect the implementation of notice transparency may have on CCPA/CPRA success in achieving California's goal of protecting consumer’s privacy.

In that connection, we write to make the following observations:

1. As introduced under §999.306 Notice of Right to Opt-Out of Sale of Personal Information, the “Opt-Out Button” as presented in §999.306(f) is linked directly to and solely associated with presenting the “Do Not Sell My Personal Information” right (DNSMPI) and choice to consumers. DNSMPI is its sole function, by definition.

This implementation fulfills the OAG’s pending requirement of 1798.185(a)(4)(C) to provide a uniform opt-out button. As a consequence, however, the “Opt-Out Button” becomes just that ... a button provided for the sole purpose of opting-out. Any use of the OOB for another purpose is confusing and at cross purposes with the regulation.

W407-1

2. Paragraphs §999.305 Notice at Collection of Personal Information and §999.307 Notice of Financial Incentive are equally foundational elements of CCPA notice transparency. Both are similar in scope and purpose to §999.306. And as a means of just-in-time briefing of consumers on privacy rights, they are equally important as the DNSMPI because:
 - Not every company collects PI from consumers.
 - Not every company that collects PI from consumers sells it.
 - Not every consumer seeking contact/category/purpose/policy information (at collection time) is interested in exercising DNSMPI rights.
 - Companies who do not sell PI (and do not display a DNSMPI) run the risk of being seen as consumer-unfriendly based on logo confusion. (“If I can’t see the DNSMPI, this must be a bad company.”)
3. From a consumer’s point of view, we believe that Notice at Collection and Notice of Financial Incentive are equally important as Notice of Right to Opt-Out in terms of consumer access. Each should be equally available and accessible at points of consumer access and PI ingress.
4. As the CCPA regulations are operationalized, there is a risk that the single-purpose Opt-Out Button as currently specified could be misunderstood and misused by companies and consumers alike to be a “CCPA privacy information button”, to be pressed for any privacy purpose. Allowing this to happen could lead to a chaotic breakdown of essential communication between companies and consumers, which should be avoided at all costs.
5. With California now in the driver’s seat for implementing privacy legislation that could form the model for many North American jurisdictions (including a national US law), we believe that the time is right for practical operational guidance to be put forward. California needs to get this right, or risk losing consumer trust for the privacy community in general.

W407-1
cont



As one means to fill this transparency “vacuum”, we suggest employing a standardized graphic framework (trigger) image at consumer touchpoints that allows companies of all sizes to guide consumers’ attention to simply organized just-in-time information covering all elements of consumer access, not just DNSMPI.

We suggest the adaptation of the Nutrition Label-style framework for this purpose. The NL paradigm readily accommodates consumers access to information under all three notice types, as well as providing single-click linked access into a company’s mother privacy policy document as a final point of reference.

A testament to the flexibility and acceptance of the NL paradigm can be seen displayed on food items of every size, description, and composition in stores everywhere. Each Nutrition Facts label lists simple facts in order of importance to consumers. A Privacy Facts label builds on that same simplicity, but leverages technology by displaying simple and concise privacy information in real time as directed by the consumer.

Use of the NL paradigm brings a number of non-CCPA benefits:

- It provides an operational means for transitioning away from the misuse of “cookie notices” and “cookie banners” as vessels for dispensing CCPA/CPRA information.
- As a national privacy law is debated in Washington, a well-conceived and implemented CCPA/CPRA notice model will attract the attention of many state jurisdictions, leading to passage of a comprehensive national law rather than a fragmented quilt of state regulations. This would be a testimony to California’s thought leadership and a large benefit to the nation’s consumers in general.
- As the US struggles for privacy adequacy with the EU and other continents, the flexibility and scope of the NL paradigm can work to promote transparency agreement across continents. Nutrition Labels are used and trusted around the world, not just in the USA.

W407-1
cont



Regarding our specific comment on the 4th set of proposed regulations, we suggest that language be added within the regulations to name the Nutrition Label paradigm as a recognized foundational tool for meeting the notice transparency requirements of CCPA/CPRA.

Additional descriptive information on practical CCPA notice implementation can be found in PrivacyCheq's previous comment submissions to the CCPA Proposed Regulation which closed on [December 6, 2019](#), [February 24, 2020](#), [March 27, 2020](#), and [October 28, 2020](#).

We thank you for these opportunities to comment.

A handwritten signature in black ink, appearing to read "D.R. Smith".

Dale R. Smith, CIPT
Futurist



W407-1
cont

From: [Mohammed, Shoeb](#)
To: [Privacy Regulations](#)
Cc: [Leder, Leslie](#)
Subject: CalChamber Comments to Fourth Proposed Modifications to CCPA Regulations
Date: Monday, December 28, 2020 2:58:51 PM
Attachments: [image001.png](#)
[CalChamber Comments to Fourth Modified CCPA Regulations.pdf](#)

Dear Lisa Kim,

Attached please find CalChamber's comments to the Fourth Set of Proposed Modifications to Text of CCPA Regulations.

Thank you,

Shoeb Mohammed
Policy Advocate
California Chamber of Commerce



December 28, 2020

SENT VIA EMAIL

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Written Comments to Fourth Set of Proposed Modifications to Text of CCPA Regulations
OAL File No. 2019-1001-05

SUMMARY

The California Chamber of Commerce (CalChamber) respectfully submits the following comments to the Attorney General’s (AG) Fourth Set of Proposed Modifications to Text of California Consumer Privacy Act (CCPA) Regulations. Recommended changes are formatted as edits to the final form of the fourth set of proposed modifications to the regulations. Recommended changes to the final form of the proposed modifications are displayed with additions in underline and deletions in ~~strikeout~~. Additionally, in Section III, we reiterate our concern that the current rulemaking activities violate the Administrative Procedures Act.

COMMENTS

- I. SECTION 999.306 – Notice of Right to Opt-Out of Sale of Personal Information.
 - A. Issue: It is unclear whether the Opt-Out Button is optional because §999.306(f)(1) conflicts with §999.306(f)(2).
 - 1. Proposed Regulation: §§ 999.306(f)

§999.306(f)(1) states the intention to make the Opt-Out Button optional by use of the term “may.” It reads, in relevant part, that the Opt-Out Button “may be used in addition to” ... “but not in lieu of any requirement to post the notice of right to opt out or a ‘Do Not Sell My Personal Information’ link.” In conflict, §999.306(f)(2) suggests that the Opt-Out Button is mandatory by use of the term “shall.” It states that the button “shall” be added where a business posts the “Do Not Sell My Personal Information” link. Accordingly, (f)(2) is in conflict with (f)(1).

Additionally, §999.306(f)(1) contains a duplicative clause that makes the regulation unclear as drafted. Subsection (1) states: “The following opt-out button may be used in addition to posting *the notice of right to opt out*, but not in lieu of any

W408-1

requirement to post *the notice of right to opt out...*” (emphasis added). The duplicative use of the clause “the notice of right to opt-out” is unnecessary and confusing. We therefore recommend deletion.

2. Recommended Changes: Revise §§999.306(f) to clarify that the Opt-Out Button is optional, and strike duplicative language for clarity, as follows:

999.306(f) Opt-Out Button

(1) The following opt-out button may be used in addition to ~~posting the notice of right to opt out~~, but not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations.

(2) Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button, should the business choose to use it, shall be added to the left of the text as demonstrated below. The opt-out button, if used, shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal information” link.

(3) The button, if used, shall be approximately the same size as any other button used by the business on its webpage.

W408-1
cont

II. SECTION 999.326 – Authorized Agent.

- A. Issue: Businesses are prohibited from using multiple forms of identity verification when requests to access consumer data come from authorized agents.

1. Proposed Regulation: §§ 999.326(a)

When a request to access or delete information comes from a party claiming to act on behalf of a consumer, a business must be permitted to use multi-step verification to ensure each request is legitimate and prevent unauthorized access. The language in the current regulations, approved by the Office of Administrative Law and effective on August 14, 2020, permits businesses to use three verification elements outlined in §999.326(a)(1)-(3) of those regulations. The proposed changes by the Attorney General initially proposed in the Third Set of Modifications, which also appear in this Fourth Set, depart from this standard, limiting businesses to only two forms of verification when three would provide additional security for consumer information.

2. Recommended Changes: Revise §§999.326(a) to allow businesses to use all three verification methods as follows:

W408-2

§999.326 Authorized Agent

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do both ~~either~~ of the following:

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

W408-2
cont

III. The Fourth Proposed Modifications Violate the Administrative Procedures Act

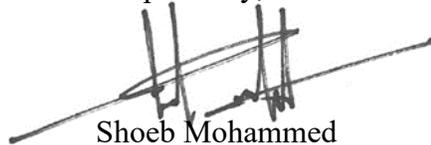
This Fourth Set of Proposed Modifications, made in response to comments to the Third Set of Proposed Modifications, is unlawful because it violates the procedural requirements of Government Code §1130 et seq, the California Administrative Procedures Act (APA).

GC 11346.4(b) provides that a Notice of Proposed Action is valid for one year. This Fourth Set of Modifications was issued in response to comments made to the Third Set of Modifications. The Third Set of Modifications was unlawful because it was published on October 12, 2020, more than one year after the original the Notice of Proposed Action dated October 11, 2019. Because 2020 is a leap year, the proposed third set was published 367 days after the original Notice of Proposed Action. Therefore, the third and fourth sets of proposed modifications are unlawful and invalid.

W408-3

CalChamber restates our comment in Section I of CalChamber's comments to the third set of proposed modifications, dated October 28, 2020. We respectfully request the Department to withdraw the third and fourth proposed sets of modifications to the text of the California Consumer Privacy Act regulations and restart a new notice period under the APA.

Respectfully,



Shoeb Mohammed
California Chamber of Commerce

From: [Jesse Vallejo](#)
To: [Privacy Regulations](#)
Cc: [Kyla Christoffersen Powell](#); [Jaime Huff](#)
Subject: Comments by the Civil Justice Association of California on Fourth Set of Proposed Regulations for the CCPA
Date: Monday, December 28, 2020 3:26:27 PM
Attachments: [image001.png](#)
[CJAC Comments CCPA Revised Regulations 12-28-20.pdf](#)

Hello,

Please find attached the comments by the Civil Justice Association of California on the fourth set of proposed regulations for the California Consumer Privacy Act.

Thank you,

Jesse Vallejo
Legislative and Communications Coordinator
Mobile [REDACTED] | www.cjac.org





CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

December 28, 2020

Xavier Becerra, Attorney General
California Department of Justice
1300 I Street, Suite 1740
Sacramento, CA 95814

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: *Comments by the Civil Justice Association of California on Fourth Set of Proposed Regulations for the California Consumer Privacy Act*

Dear Attorney General Becerra:

The Civil Justice Association of California ("CJAC") appreciates the opportunity to provide comments on this latest version of the proposed regulations implementing CCPA.

CJAC respectfully requests the Office of the Attorney General address the following issues:

1. Clarify that use of the opt-out button is optional since it is duplicative and may be confusing.

The proposed Section 999.306(f) indicates the opt-out button is optional at the outset but then follows with language suggesting it is mandatory. Subsection (f)(1) states the opt-out button "**may** be used in addition to a notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a 'Do Not Sell My Personal Information' link" (emphasis supplied). However, subsection (f)(2) states that "Where a business posts the 'Do Not Sell My Personal Information' link, the opt-out button **shall** be added to the left of the text" (emphasis supplied).

We request clarification the button is optional. It appears that (f)(2) is mandating the position of the button only, but the language is unclear. Since the notice of right to opt out or a "Do Not Sell My Personal Information" ("DNS") link is required regardless, the button is duplicative and could also be confusing. Some consumers may believe that merely clicking the toggle-like button effectuates the opt-out, when the button is just another link to the DNS page. In light of this, it is best left to the business to decide whether the button will facilitate the opt-out process on a given web page. We also suggest providing flexibility to businesses with the design and placement of the button, as businesses may find approaches that are simpler and clearer for the consumer.

W409-1

Accordingly, we recommend revising subsections 999.306(f)(1) and (2) as follows:

(f) Opt-Out Button.

(1) The following opt-out button **or one that is similar** may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link as required by Civil Code section 1798.135 and these regulations. **Businesses are not required to use an opt-out button.**

(2) ~~Where~~ **When** a business **chooses to use the opt-out button with** posts the “Do Not Sell My Personal Information” link, the opt-out button shall be added to the left of **next to** the text, **similar to what is as** demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link.

W409-1
cont

(3) The button shall be approximately the same size as any other buttons used by the business on its webpage.

2. Allow businesses to request two forms of identity verification from authorized agents to provide better protection of consumers.

CJAC requests the below language be revised per the below to allow businesses to require two forms of identity verification from authorized agents, which will provide stronger protection of consumers and their information from fraudsters:

§ 999.326 Authorized Agent.

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request **along with two forms of identity verification**. The business may also require the consumer to do either of the following:

W409-2

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

3. Provide a reasonable implementation period for the latest revisions.

Given the complexity and burden of implementing new regulations, which has been further exacerbated by remote workforces and shutdowns, we ask the Attorney General to specify in the regulations that businesses have at least six to 12 months from final adoption of the regulations to implement them before they are enforced. This will also provide certainty businesses need, especially during these times.

W409-3

Conclusion

Addressing the forgoing concerns will help reduce unnecessary enforcement and litigation burdens on businesses, the courts, and your Office. We are happy to answer any questions you may have and look forward to the opportunity to work with your Office on improvements to the regulations.

Thank you for your consideration,



Kyla Christoffersen Powell
President and Chief Executive Officer

From: [Lisa LeVasseur](#)
To: [Privacy Regulations](#)
Subject: Comments on Fourth Round of amendments
Date: Monday, December 28, 2020 3:37:10 PM
Attachments: [CCPA Fourth Round Comments.pdf](#)

Dear Ms. Kim,

Please find our written comments on the fourth round of amendments to the CCPA attached.

Warmly,

Lisa LeVasseur

Executive Director, Me2B Alliance



401 Edgewater Place
Suite 600
Wakefield, MA 01880

December 28, 2010

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Re: *OAL File No. 2019-1001-05: NOTICE OF FOURTH SET OF PROPOSED
MODIFICATIONS TO TEXT OF REGULATIONS AND ADDITION OF DOCUMENTS
AND INFORMATION TO RULEMAKING FILE*

Dear Ms. Kim:

Thank you for the opportunity to submit comments in response to the fourth set of proposed modifications made to the regulations regarding the California Consumer Privacy Act (CCPA).

The Me2B Alliance is a non-profit organization founded in 2019 with a mission of performing independent product testing/certification on connected technology—essentially measuring the ethical behavior of technology. Our primary ethos is that *respectful technology* is better for both people (“Me-s”) and businesses (“B-s”). Our ethical foundation for *respectful technology* lies in what we call the Me2B Rules of Engagement, which mirror the attributes of healthy human inter-personal relationships.

Why use the characteristics of healthy human relationships as an ethical north star? Because we *are* in relationships with connected technology: it observes us, talks to us, interacts with us—just like people. When technology treats us with respect, it engenders greater trust in connected products and services, and the companies that provide them.

A crucial principle in the Me2B Rules of Engagement is *Respectful Defaults*:
Respectful Defaults - *In the absence of stated preferences, we default to the most conservative behavior.*

Note this also aligns with the Privacy by Design principle: “Privacy as the default setting.”ⁱ
In particular, we strongly suggest that opting-in to information sharing or selling should

be the default standard for Web interactions; it reflects a more respectful default than requiring people to opt-out.

General Problems with Opting-Out

The current opt-out mechanism is problematic on multiple fronts:

1. It only applies to the “sale” of user data and not to sharing of user data, even though portable data can be shared with a service provider, who could sell the data without any notice or consent.
2. It places the burden on the individual to, in essence, opt-in to privacy, which fails to align with the human right of privacy; it also fails the principle of privacy as the default setting in Privacy by Design.
3. It presents significant difficulty in developing a global privacy signal standard, as the European Union in recent decisions has made clear that opt-out is not GDPR compliant.
4. Opting-Out presents a particularly confusing user interface (UI) in communicating a negative/opt-out (see also comments below regarding section 999.315).

W410-1

In addition to the general comments above, the Alliance would like to submit its views on two discrete but important proposed changes to the draft regulations.

1. 999.306(b)(3): “sells” versus “collects”

Revisions to section 999.306, subd. (b)(3) would “clarify that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of the sale of their personal information by an offline method.”

Part of this revision would alter the language in (b)(3) to cover a business that “sells” personal information, rather than “collects” such data from consumer.

W410-2

This language change is troubling on several fronts. First, it greatly narrows the scope of covered interactions with consumers. Clearly “selling” is a subpart of data “collecting”. Or to be more precise, “selling” is a specific use of data after the act of “collecting.” We believe all people should be notified of information collection whether it’s intended to be “sold” (CCPA definition) or used strictly in the context of the vendor/first party. This is particularly important during the national COVID pandemic, with known mobile data sharing from SDKs installed in apps, which are being shared through service provider loopholes and then sold by subsequent parties in the data supply chains without notice to users.

Second, “selling” is a more ambiguous term than “collecting.” A company theoretically could evade the assumed intent of the provision by adopting a cramped definition of selling data.

Third, allowing data collection, even in the absence of sales, increases security risks for the user. Collection of data entails storing it on third party servers, where it would be subject to outside breaches and other harms.

Finally, while CCPA mostly restricts the “sale” of user data, and the newly-passed CPRA expands to restrict the “sharing” of user data, these two conflicting standards, without any technical consent-sharing mechanisms, present an impossible scenario for end-users or auditors to track the flow of their user data, and ensure that portable data isn’t sold by parties who legally acquired the ‘shared’ user data under CCPA frameworks.

W410-2
cont

2. 999.315(f): the “opt-out button”

Proposed section 999.315, subd. (f) describes a uniform button (or logo) to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

Usability Issues with Opt-Out

Based on the findings of Cranor et al (listed as a resource in this round of proposed changes) which recommends an interactive simple text statement (“do not sell my data”) without an icon as the most understandable UI per their testing, we are surprised to see the recommendation of an (untested?) generic checkmark icon.

From Cranor et alⁱⁱ:

“None of the tested icons should be used to symbolize Do Not Sell. Instead, the link text should be used on its own or different icons should be developed and tested.... adding any of these icons to the link text introduced misconceptions regarding the opt-out button’s purpose compared to presenting the link text on its own.”

W410-1
cont

It should be noted that the four icons tested by Cranor et al were all significantly more meaningful than the proposed check-mark button proposed in this revision.

In fact, using a checkmark with a negative statement sets up a particularly challenging UI for people, which is well understood in the art of UI designⁱⁱⁱ.

Additionally, in another listed resource, “An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites”^{iv}:

“In asking for consent, websites should present a clear, affirmative action, and ask visitors for agreement rather than incorporating the consent into default settings, such as pre-checked boxes (Art. 4).”

We contend that mandating opting-out of selling data is tantamount to a default setting allowing the selling of data. Instead, people should be presented with a clear, affirmative [opt-in] action to *allow* the selling of their data.

Location of Opt-Out Signal on Infinite Scroll Pages

Furthermore, the suggested practice under CCPA to place a “Do Not Sell My Information” link in the footer of websites, is not possible for websites with “infinite scrolling” functionality, where new stories or content constantly populates as soon as a user scrolls to the bottom of the page where the footer links exist^v. This concept also doesn’t work on publishers with paywalls – where a user visits a page and is immediately both tracked and identified by javascript pixels on the page, but also unable to click on any elements besides the subscription notices to execute an effort to opt-out of any data sales. GDPR on the other hand, approaches consent from a position where a website can’t use UI/UX tricks, locked-in pop-ups, infinite scrolling and other “scroll & click tricks” to collect consent or make it possible to opt-out. By making this “opt-out” instead of “opt-in,” many users must sometimes navigate purposefully-broken websites that restrict clicks, scrolling, engagements (newspaper paywalls) and prevent users from being able to express their lack of consent for data sales.

W410-1
cont

Users Are Less Likely to Change Default Settings

Requiring people to opt out of selling their data is essentially a default setting that allows vendors to sell the data of users. Research shows that default settings favor whoever benefits from the default setting.

“The same applies to privacy settings, researchers [have found in several studies](#).

“Several possible reasons for not changing the default settings exist: cognitive and physical laziness; perceiving default as correct, perceiving endorsement from the provider; using the default as a justification for choice, lacking transparency of implication, or lacking skill,” researchers from the Goethe University Frankfurt and Nelson Mandela Metropolitan University [wrote in 2013](#).”^{vi}

“If we assume that marketers, consumers, and policy-makers all share the goal of separating interested from uninterested consumers, our findings suggest some constructive advice regarding the role of defaults. In our research, defaults have a sizable effect, and the best way of controlling these effects may well be to neutralize them as much as possible.”^{vii}

Changing to a Positive Statement

If we were to modify the confusing negative language of the proposed “Do Not Sell” button and instead reword it in a positive manner it would essentially be, “I want data privacy”. This option should be tested and considered.

Opting-In Better Aligns with Judicial Opinions in the EU

Due to the maturity of the GDPR (relative to the CCPA), consent mechanisms have been more deeply scrutinized and tested in the European Union. Consent for data usage must be provided by “clear affirmative action”--i.e. opt-in. Whereas in the CCPA, the individual is defaulted into allowing the sale/sharing of information until they opt-out. The EU and Germany have upheld support for opting-in in the past year, affirming that opt-out is *not* valid consent.

From the Court of Justice of the European Union, October 2019^{viii} [bold text below for emphasis and focus, not from original source]:

*“In today’s judgment, the Court decides that the **consent** which a website user must give to the storage of and access to cookies on his or her equipment **is not validly constituted by way of a prechecked checkbox which that user must deselect to refuse his or her consent.**”*

From the related case, May 28, 2020, the German Federal Court of Justice (*Bundesgerichtshof*, “BGH”) decided on the “Planet49” case regarding cookies^{ix}:

*“The BGH ruled that Section 15 para. 3, sentence 1 TMA must be interpreted in light of and in conformity with Art. 5 para. 3 of the ePrivacy Directive as meaning that the use of cookies for creating user profiles for the purposes of advertising or market research **requires the user’s consent**. Following the decision of the CJEU, the BGH **further ruled that the user’s consent cannot be obtained by way of a pre-ticked checkbox which the user can uncheck.**”*

And from the UK’s ICO (Information Commissioner’s Office), “Consultation: GDPR consent guidance”, March 31, 2017^x:

W410-1
cont

“Clear affirmative action means someone must take deliberate action to opt in, even if this is not expressed as an opt-in box. For example, other affirmative opt-in methods might include signing a consent statement, oral confirmation, a binary choice presented with equal prominence, or switching technical settings away from the default.

The key point is that all consent must be opt-in consent – there is no such thing as ‘opt-out consent’. Failure to opt out is not consent. You may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way.”

Opting-In Eases Global Privacy Signal Standardization Efforts

Changing from opt-in to privacy to opt-in to selling/sharing data will align this important regulation more closely to the EU approach, which will facilitate the development of a global privacy signal standard. Currently, there is effort in the W3C to develop a global standard for a Global Privacy Control signal that is facing difficulties with reconciling a signal and a default setting that works everywhere.

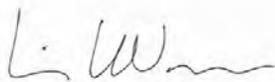
Recommendation

For the reasons stated above we strongly recommend changing the default from an opt-out of selling my data to opt-in to selling my data. Doing so will result in a privacy-respecting and Privacy by Design-compliant default, an easier to understand user-interface, and an easier path to a global privacy signal standard.

In the absence of this, positive language of the control/button (or logo) such as, “I want data privacy” (yes/no) should be evaluated.

On behalf of the Me2B Alliance, thanks again for the opportunity to provide feedback on this important regulation for California, the US and the world.

Sincerely,



Lisa LeVasseur
Executive Director, Me2B Alliance

ⁱ https://en.wikipedia.org/wiki/Privacy_by_design

ⁱⁱ "CCPA Opt-out Testing – Phase Two", Cranor, Habib, et al, May 28, 2020. [CCPA Opt-Out Icon Testing - Phase 2 - DNS \(ca.gov\)](#)

ⁱⁱⁱ [Checkboxes - Checkbox label negating - User Experience Stack Exchange](#)

^{iv} "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites", Habib, Zou et al, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019. August 11–13, 2019, Santa Clara, CA, USA.

^v <https://oag.ca.gov/data-broker/registration/193828>

^{vi} "Default settings for privacy -- we need to talk" Albert Ng, December 21, 2019, CNET. [Default settings for privacy -- we need to talk - CNET](#)

^{vii} Defaults, Framing and Privacy: Why Opting In-Opting Out¹ (columbia.edu) Defaults, Framing and Privacy: Why Opting In-Opting Out

^{viii} "Storing cookies requires internet users' active consent", Court of Justice of the European Union PRESS RELEASE No 125/19 Luxembourg, 1 October 2019 Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband eV v Planet49 GmbH.

^{ix} "Germany: The decision of the German Federal Court of Justice on cookie consent – and further implications", *Global Compliance News*, Julia Kaufman, July 19, 2020. [Germany: The decision of the German Federal Court of Justice on cookie consent - and further implications \(globalcompliancenews.com\)](#)

^x "Consultation: GDPR consent guidance", Information Commissioner's Office, March 31, 2017. [draft-gdpr-consent-guidance-for-consultation-201703.pdf \(ico.org.uk\)](#)

From: [Jacob Snow](#)
To: [Privacy Regulations](#)
Subject: Privacy and Consumer Organization Comments on Proposed CCPA Rulemaking
Date: Monday, December 28, 2020 3:53:15 PM
Attachments: [2020.12.28 - Fourth Coalition Comments re OAG Regs.pdf](#)

Attached are comments from a coalition of privacy and consumer protection organizations regarding the Fourth Set of Modifications to Proposed Regulations under the California Consumer Privacy Act.

Best,

Jake Snow
Technology and Civil Liberties Attorney
ACLU of Northern California
he/him/his | [REDACTED] | @snowjake

Comments to the
California Office of the Attorney General

Notice of Fourth Set of Modifications
to Proposed Regulations under
The California Consumer Privacy Act

Submitted via Email to PrivacyRegulations@doj.ca.gov

December 28, 2020

On Behalf of the Following Organizations:



The “Do Not Sell My Personal Information” Icon Will Help Ensure That Californians Are Made Aware of Their Privacy Rights.

The undersigned organizations sincerely appreciate your ongoing efforts to establish a workable, standardized icon to signal to consumers their right to opt-out of the sale of their personal information under the California Consumer Privacy Act.

The proposed icon is an improvement on the icon recommended in earlier drafts of the regulations, and more clearly conveys the presence of privacy choices. Testing by Professor Lorrie Faith Cranor and the CyLab Security and Privacy Institute at Carnegie Mellon University demonstrated that any icon divorced from an accompanying tagline is likely to be misinterpreted by consumers.¹ This icon and the “Do not sell my personal information” tagline will help ensure that Californians are made aware of their privacy rights.

Condensing the universe of concepts associated with privacy, choice and specifically the sale of personal information to a single, standardized icon is a monumental challenge. In responding to the issues we've raised in previous comments, your Office has demonstrated a commitment to developing workable solutions to the most difficult policy areas of the California Consumer Privacy Act. We remain hopeful that, despite the unavoidable potential for this icon to be misconstrued, these regulations will build broad public awareness and help make the privacy-choices icon iconic.

Signed:

American Civil Liberties Union of California

Common Sense Kids Action

Electronic Frontier Foundation

Privacy Rights Clearinghouse

¹ Cranor, *et al.*, CCPA Opt-Out Icon Testing – Phase 2, p.5 (May 28, 2020).

From: [Halpert, Jim](#)
To: [Privacy Regulations](#)
Cc: [Kingman, Andrew](#)
Subject: State Privacy & Security Coalition -- Comments re AG's Office CCPA 4th Modified CCPA Rules December 28 2020.DOCX
Date: Monday, December 28, 2020 5:07:33 PM
Attachments: [State Coalition -- Comments re AG s Office CCPA 4th Modified CCPA Rules December 2u 2020.DOCX](#)

Dear Ms. Kim,

Attached are the State Privacy & Security Coalition's comments on the latest version of the proposed CCPA rule revisions.

We would very much appreciate your office reviewing the entirety of these comments carefully.

Respectfully submitted – Jim Halpert

Jim Halpert
Partner

T
M

DLA Piper LLP (US)
dlapiper.com
<https://www.dlapiper.com/en/us/people/h/halpert-jim/?tab=credentials>

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

STATE PRIVACY & SECURITY COALITION

December 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Department of Justice
300 Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Comments Regarding Title 11(1)(20): Fourth Set of Proposed Modification of Text of Regulations

I. Introduction

The State Privacy & Security Coalition is a coalition of 29 companies and 7 trade associations across the retail, payments, communications, technology, fraud prevention, tax preparation, automotive and health sectors. We work for laws and regulations at the state level that provide strong protection for consumer privacy and cybersecurity in a consistent, workable manner that reduces consumer confusion and unnecessary compliance burdens and costs.

Our Coalition worked with Californians for Consumer Privacy and consumer privacy groups on amendments to clarify confusing language in the CCPA, to reduce the risk of fraudulent consumer requests that would create risks to the security of consumer data, and to focus CCPA requirements on consumer data, consistent with the title of the law.

We appreciate the clarifications that the 4th modifications have made to the examples in § 999.306(b) that align them much more closely with the requirements of the statute and avoid significant potential consumer confusion.

W412-1

On the other hand, we remain very concerned that proposed § 999.326(a) would seriously weaken authentication of authorized agents when they ask to exercise right to know and data deletion rights on behalf of state residents and result in a material increase in California residents' exposure to account takeovers from fraudulent authorized agent requests. We understand that your office is not requesting comments on this issue, but urge you to review our comments below, as they more fully explain the risks to privacy associated with the proposed changes to § 999.326(a).

W412-2

In addition, the “do not sell” icon that is now proposed in § 999.306(f) is not well-designed “to promote consumer awareness of the opportunity to opt-out of the sale of personal information” and should instead be developed per the procedures set forth in § 1798.185(a)(4)(C) of the CPRA, instead of being thrust into the CCPA regulations at this late juncture. Furthermore, the language in § 999.306(f)(2) is ambiguous and should be clarified, if this provision is incorporated in the next version of final rules.

W412-3

W412-4

STATE PRIVACY & SECURITY COALITION

1. The proposed restriction in § 999.326(a) on authenticating third party right to know and data deletion requests should be clarified or stricken in the final rule to reduce risk of pretexting and fraud.¹

Right to know and data deletion requests pose greater data security risk because they allow a fraudulent requester to obtain personal data, or delete or otherwise manipulate account information and potentially hijack the account. The Final Rules impose greater authentication requirements for right to know and data deletion requests because of the heightened security and privacy risks these rights pose if wielded by fraudsters or hackers.

These very same risks counsel strongly against cutting back on businesses' leeway to authenticate right to know and data deletion requests filed by a purported authorized agent.

We are unclear about the rationale for shifting the submission of proof of the signed permission authorizing the agent from the consumer to the authorized agent. While the addition of such an option might be workable, allowing a business to do only one (and not both) of further authentication steps risks increased fraud.

We request the following amendment to § 999.326(a), as follows:

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do ~~either of do~~ the following:

A business should not be barred from both asking the consumer to verify their identity with the business *and* obtaining confirmation that the consumer provided the agent permission to submit the request. Both pieces of information are necessary to confirm that a request is not fraudulent. Otherwise, a fraudster can either: (1) submit a request in the name of an actual consumer who has not authorized the request, or (2) create a fake account in the same name as an actual consumer, thereby making the fake account appear more real, but submit the access or deletion request for the actual consumer's account. For these reasons, both confirmations are *very important* to prevent fraudulent requests for these rights that, as the final regulations acknowledge, pose greater risks to consumers.

2. The Proposed Icon is Premature and Should Be Addressed in the CPRA Rulemaking

The CPRA requires a rulemaking in the next [18 months] that will establish a process to select an effective icon. Selecting an icon without any procedure for doing so is unwise because a consumer testing process is the best way to ensure that the icon is understood and provides a clear, positive user experience. Furthermore, establishing the icon now would either preempt the process approved by the

¹ This section contains a more detailed explanation of risks associated with the proposed revision to this section and we respectfully request that your Office review this section of our comments even though the latest version of the proposed rules does not make a change to the previous proposal.

STATE PRIVACY & SECURITY COALITION

voters, or would result in a second icon being chosen under the CPRA development process, needlessly confusing California consumers.

The proposed rules are actually the *seventh* proposed version of CCPA rules. These repeated changes needlessly complicate CCPA compliance during an economic downturn and in the case of a second icon, would defeat the purpose of branding a symbol of how to exercise the CCPA do not sell right.

W412-3
cont

For all these reasons, it is better to wait, remove this provision, and follow the CPRA process in selecting the icon.

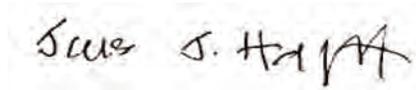
However, if the Attorney General's Office decides to add a "do not sell" icon provision, it should clarify the language in proposed § (f)(2), to make clear that the location requirements apply, "If the business posts the icon." This could be accomplished by amending the text as follows:

(2) If a business posts the icon, it shall ~~Where a business posts the "Do Not Sell My Personal Information" link, add~~ the opt-out button ~~shall be added~~ to the left of the location text where a business posts the "Do Not Sell My Personal Information" link, as demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" link.

W412-4
cont

This change would avoid potential confusion between the text of paragraph (1), which states that posting the icon is voluntary, and paragraph (2) which prescribes where to post the icon, but could be read as requiring that the icon be posted in all cases. Mandating use of the icon without user testing and the process to be developed under the CPRA would compound the problems posed by hasty implementation of the icon.

Respectfully submitted,



Jim Halpert, Counsel
State Privacy & Security Coalition

CCPA Opt-Out Icon Testing – Phase 2

May 28, 2020

Lorrie Faith Cranor, Director of CyLab Security and Privacy Institute, Bosch Distinguished Professor in Security and Privacy Technologies, FORE Systems Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University (lorrie@cmu.edu)

Hana Habib, PhD Candidate, School of Computer Science, Carnegie Mellon University (htq@cs.cmu.edu)

Yaxing Yao, Postdoctoral Associate, School of Computer Science, Carnegie Mellon University (yaxingyao@cmu.edu)

Yixin Zou, PhD Candidate, School of Information, University of Michigan (yixinz@umich.edu)

Alessandro Acquisti, Trustees Professor of Information Technology & Public Policy, Carnegie Mellon University (acquisti@andrew.cmu.edu)

Joel Reidenberg, Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University School of Law (jreidenberg@fordham.edu)

Norman Sadeh, Professor of Computer Science and Co-Director Privacy Engineering Program, Carnegie Mellon University (sadeh@cs.cmu.edu)

Florian Schaub, Assistant Professor, School of Information, University of Michigan (fschaub@umich.edu)



Table of Content

Executive Summary	2
1. Introduction	4
2. Methodology	4
2.1 Evaluation Method	4
2.1.1 Attention	5
2.1.2 Intention to Click	6
2.1.3 Communication of “Do Not Sell”	6
2.1.4 Icon Preferences	7
2.2 Participants	7
2.3 Data Analysis	8
3. Results	8
3.1 Attention	9
3.1.1 Less than Half Could Accurately Recall Seeing the Do-Not-Sell Icon/Link	9
3.1.2 “PriceTag” and “StopSign” Performed the Best in Drawing Attention	11
3.2 Communication of “Do Not Sell”	12
3.2.1 Correct Expectations Related to Do-Not-Sell Are Common	12
3.2.2 No Icon Performed Best in Creating the Expectation of Do-Not-Sell Choices	14
3.2.3 Potential Misconceptions Generated By Icons	15
3.3 Icon Preferences	15
3.3.1 “DoNot” and “Person” Favored for Conveying “Do-Not-Sell” Concept	15
3.3.2 All Icons Conveyed Inaccurate Information When Viewed Alone	16
3.3.3 Most Icons Failed to Convey the Concept of Personal Information	18
3.3.4 Icons Only Make Sense When Accompanied by the Link Text	19
3.4 Intention to Click	19
3.4.1 Participants Exhibited High Intentions to Click	19
3.4.2 Top Reasons for Intending to Click	20
3.4.3 Top Reasons for Intending not to Click	20
3.6 Recognizability at a Small Scale	21
3.5 Comparison with Previous Findings	21
4. Conclusions	23
References	24
Appendix A: Survey Questions	26
Appendix B: Participant Demographics	31
Appendix C: Codebook	33

Executive Summary

Following our prior user studies on the effectiveness of icons and link texts for the CCPA do not sell opt-out button [1,2] , we tested the following set of candidate icons proposed by the California Attorney General’s office (OAG) with a demographically-diverse sample of 1,002 California residents. We explored which of these icons, paired with the “Do Not Sell My Personal Information” link text, would perform best in (1) standing out to users on a website; (2) communicating the presence of a do-not-sell choice; and (3) motivating users to click. We also included a control condition (*None*) in which just the text link was shown to participants, to explore whether the presence of an icon had an impact.



Figure 1: Icon conditions tested in our study.

Based on the results of the test we make the following recommendations:

None of the tested icons should be used to symbolize Do Not Sell. Instead, the link text should be used on its own or different icons should be developed and tested. Our analysis of the icon’s ability to communicate “Do Not Sell” indicates that showing the link text without any icon resulted in the highest percentage (64%) of correct expectations of what would happen when it is clicked - i.e., being presented with information or choices related to do-not-sell. When the link text was paired with any of the four icons, the percentage of correct expectations was lower, between 56% to 59% (Section 3.2.1). This means that adding any of these icons to the link text introduced misconceptions regarding the opt-out button’s purpose compared to presenting the link text on its own. Additionally, none of the four icons were rated particularly well by participants as conveying “there is an option to tell a website ‘do not sell my personal information’” (Sec. 3.3).

Our study shows that adding an icon did increase users’ attention (Sec. 3.1) but did not create a significantly higher motivation to click (Sec. 3.4.1). If an icon is to be used, there might be better icon designs beyond those tested here that may generate correct expectations of the opt-out button’s purpose. For instance, in our previous reports [1,2] we showed that a blue stylized toggle icon effectively communicates the presence of a choice; when paired with the “Do Not Sell My Personal Information” link text, it helps people recognize that the choice is related to the sale of personal information without creating substantial misconceptions (Sec 3.6). However,

further testing is needed to determine whether this or other alternative icons would stand out on a website or motivate users to click.

Public education is needed to raise awareness and dispel misconceptions. It is important to note that regardless of whether and which icon is adopted, consumers should be educated about the existence of the do-not-sell opt-out, how it is represented on websites, and where to find it on websites. Furthermore, it is important to educate consumers about the purpose of the opt-out button and what to expect when they click it. Our participants reported that candidate icons conveyed a variety of concepts other than “do not sell my personal information,” for example, sales, money, and payment (Table 3). Clarifying that the icon/link would lead to actual controls to stop the website/company from selling the consumer’s personal information is also helpful for persons who are unmotivated to click because they are unfamiliar with the icon and thus question its legitimacy (Sec. 3.4.3).

1. Introduction

In February 2020, we submitted a report to the OAG that documents our user research on the effectiveness of different icon and tagline (or link text) combinations for communicating the presence of Do-Not-Sell choices [1]. This choice is required to be made available to California consumers under the California Consumer Privacy Act (CCPA). Our recommendations inspired the proposed do-not-sell opt-out button in the OAG’s February 10, 2020 Revised Proposed Regulations (§ 999.306.f) [3], which was similar to, but not exactly like, the blue toggle icon we had recommended [1]. In a follow-up report [2], we presented empirical evidence showing that the OAG’s proposed toggle icon was often misinterpreted as an actual toggle control, and did not effectively convey a do-not-sell choice. In light of these findings, the OAG removed the opt-out button from the March 11, 2020 Revised Proposed Regulations, leaving the requirement to include the “Do Not Sell My Personal Information” link text [4].

At the request of the OAG, we conducted a follow-up experiment to evaluate four icon designs proposed by the OAG (shown in Figure 1) and compare them with a control condition in which the “Do Not Sell My Personal Information” link text is displayed without an icon. The OAG’s icons are closely based on icon designs developed and evaluated in our prior studies [1,2].

The experiment discussed in this report aims to answer the following three questions for each of the candidate icons provided by the OAG, using a similar methodology as in our previous studies [1,2]

1. Does this icon, when coupled with the link text, stand out to consumers on a website?
(attention)
2. Does the icon, when coupled with the link text, indicate “Do Not Sell My Information”?
(communication of “Do Not Sell”)
3. Does this icon, when coupled with the link text, motivate consumers to take action/click?
(intention to click)

2. Methodology

We conducted an online study using the Qualtrics survey tool with 1,002 demographically-diverse California residents recruited on Amazon Mechanical Turk.¹ Each participant was shown the front page of a website for a fictitious online shoe retailer that included the “Do Not Sell My Personal Information” link text near the bottom of the page. Participants were randomly assigned to one of five conditions, in which one of the four candidate icons or no icon was placed to the left of the link text.

¹ See <https://www.mturk.com/>

2.1 Evaluation Method

The study consisted of the following four parts, presented in the following order: the first three parts included questions evaluating participants' attention, intention to click, and each icon's ability to communicate the "do not sell" concept; the fourth part captured participants' opinions on all four icons.² The study concluded with questions about participants' familiarity with CCPA and demographic information. We adopted similar questions as in our previous testing [1,2], with new questions that aim to gauge participants' attention to and intention to click on the icon.

2.1.1 Attention

Participants were shown a screenshot of a fictitious shoe retailer website called "Footwear," with the icon and link text placed in the footer under the link to the website's privacy policy, to mimic the way users are likely to encounter a CCPA opt-out in the real world (see Figure 2).

Participants were first asked: "Imagine you were shopping at this online store and you wanted to know whether you could have a pair of shoes shipped to you overnight. Do you see a link you could click to find out?" Participants who said "yes" were prompted to describe the link. The correct answer, "Delivery Information," was placed two lines above the "Do Not Sell My Personal Information" link³. In this way, we directed participants' attention to the bottom right of the page without priming them to actively look for the do-not-sell icon and link.

Next, we hid the screenshot and asked participants: "Imagine you were shopping at this online store, and you were concerned about the store selling your personal information. Do you remember seeing any feature in the screenshot that you could use to prevent this from happening?" Participants who said "yes" were prompted to describe the feature. This question was designed to determine whether the link text on its own or in combination with an icon stands out enough to attract the attention of website visitors who are reviewing the website footer, but not specifically looking for this link. We analyzed each response to see whether the participant correctly described at least one of the following: the icon (e.g., "a red symbol"), the link text (e.g., "do not sell my personal information" or similar phrases such as "do not sell my info"), or the icon/link text location (e.g., "a line of text on the lower right side of the screen").

Finally, we showed the screenshot again and asked participants the same question and follow-up. This question was designed to determine whether participants were able to locate the do-not-sell icon and link text when given explicit instructions.

² The full set of survey questions for this study are included in Appendix A.

³ Arguably, other answers such as "Contact" might offer valid ways of determining the availability of overnight shipping. However, we focus on participants who included "delivery" in their response to ensure participants were looking at the bottom right corner of the page.

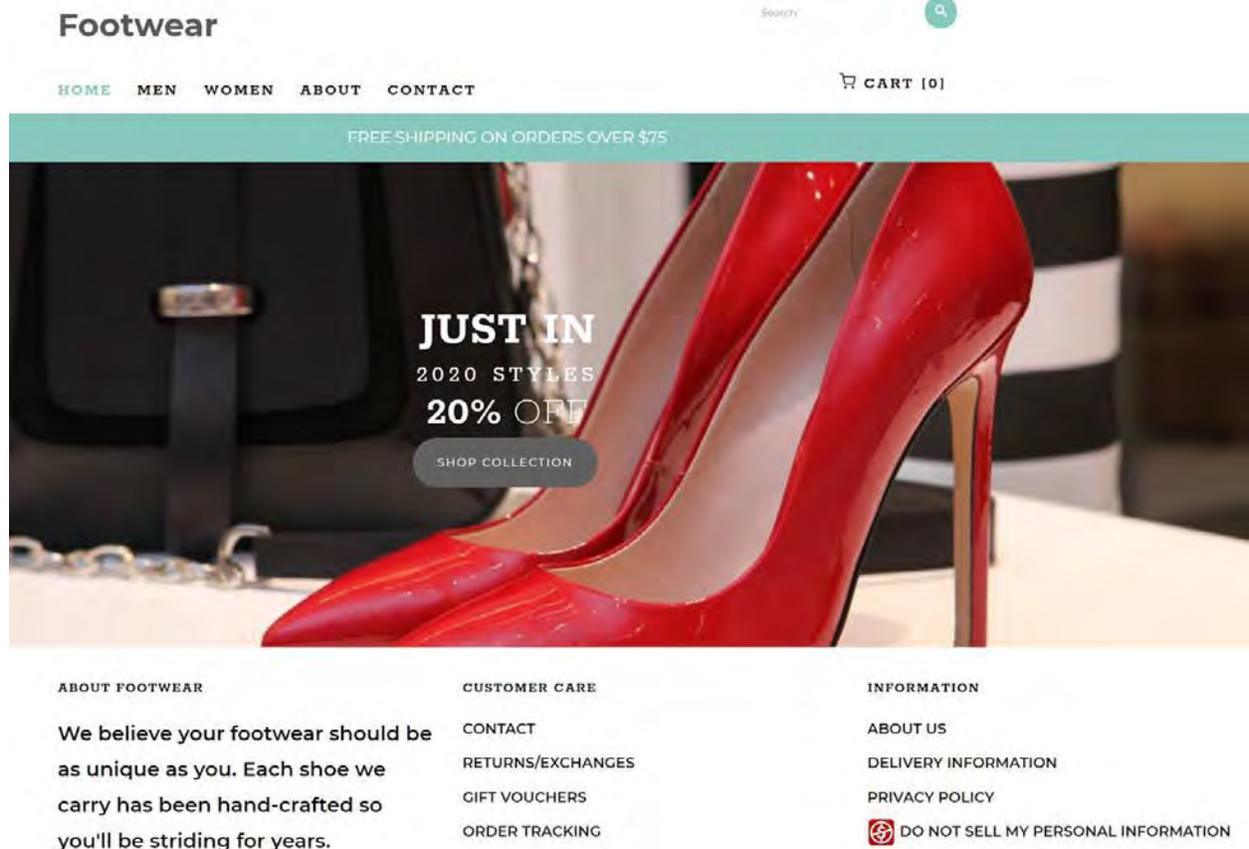


Figure 2: Screenshot of what participants assigned to the condition “DoNot” saw within the survey platform Qualtrics.

2.1.2 Intention to Click

We showed participants the screenshot again, this time with an orange box around the icon and link text, as well as a close-up of just the icon and link text, to ensure that all participants focused on the correct opt-out button/link. We asked participants to imagine this was the first time that they noticed this icon and link text on this or any other website, and to report whether they would “definitely not,” “probably not,” “not sure,” “probably,” or “definitely” click on the icon and link text. We emphasized “this or any other website” to ensure their responses were not too constrained to this specific shoe website, but instead applicable to other types of websites as well. We then asked them to describe why they selected a particular answer option to better understand their reasons for clicking and not clicking.

2.1.3 Communication of “Do Not Sell”

We asked participants to describe their expectations of what would happen if they clicked on the icon and link text shown in the orange box on the website screenshot. After that, we asked them

to rate the likelihood regarding each of eight specific scenarios about what might happen if they click the link. These scenarios were based on open-ended responses provided by participants in our previous studies [1,2]. Three of these scenarios were accurate expectations related to do-not-sell - i.e., after clicking, the user would be taken to a page where they could choose whether or not the website can sell their personal information, confirm that they do not want their personal information to be sold, or read more information about how the website uses and shares their personal information. The other scenarios were various potential misconceptions - i.e., after clicking the user would be taken to ads about privacy and security products, sales/discounts/free stuff, payment options, or the clicking would give the website permission to sell their personal information or cause the website to send unwanted emails. For each scenario, we asked participants to indicate whether it is “definitely not,” “probably not,” “not sure,” “probably,” or “definitely” going to happen.

2.1.4 Icon Preferences

After answering questions for just one icon (or link text without an icon), participants were shown all four candidate icons in randomized order. For each icon, they were asked to rate how well the icon conveys that there is an option to tell a website “do not sell my personal information,” with choices “I don’t know,” “not at all,” “slightly,” “moderately,” “very well,” or “extremely well.” They were then asked to explain the rationale behind each rating. By doing this, we provided participants an opportunity to elaborate on their opinion on design elements within each icon, as well as compare different icons.

2.2 Participants

We launched the study in April 2020 on Amazon Mechanical Turk (MTurk). MTurk is a crowdsourcing platform used by many academic researchers for recruiting participants, and prior research has shown that MTurk is a reliable data source for understanding people’s security and privacy knowledge and experiences [5]. Participants who were 18 years old or older, have completed more than 500 assignments on MTurk,⁴ with a 95% or higher approval rate were eligible to take our study. Additionally, at the request of the OAG, we used MTurk’s U.S. region targeting feature to exclusively recruit participants who lived in California according to their MTurk profiles. Because some participants’ current residence might be different from what they reported to MTurk (e.g., when they moved to a different state), we also asked participants in which state they currently reside, and we only included those who reported living in California in our data analysis. Participants were compensated \$2.50 for completing the study which took 5 to 15 minutes to complete (mean: 11.7 minutes, median: 10.0 minutes, standard deviation: 6.6), in line with California’s minimum wage (\$12/hour). Compensation to participants was funded by the OAG.

⁴ Due to the limited number of eligible participants, we lowered the requirement to “number of completed HITs > 100” after the first 409 participants, and further dropped the number of completed HITs requirement after the first 763 participants.

After removing 192 participants who provided low quality responses (i.e., including nonsensical text to one or more open-ended questions) and 93 participants who provided reasonable responses but self-reported living outside of California, we analyzed the remaining 1,002 valid responses. Responses were almost evenly distributed across the five conditions (*DoNot*: 198, *Person*: 202, *PriceTag*: 201, *StopSign*: 201, *None*: 199).

The demographic information we collected indicates that our sample was fairly diverse, but not perfectly representative of California residents when compared to U.S. census data [6,7,8].⁵ Compared to California's population, our participants were younger (63.6% were 25 to 44 years old, versus 28.6% for the CA population), more educated (69.0% having a Bachelor's/Associate's degree or above, versus 42.2% for the CA population), with a higher representation of men (50.4%, versus 49.7% for the CA population) and Asians (22.3%, versus 15.3% for the CA population). Our participants were distributed among the six California regions in roughly the same proportion as the California population; 20.7% of participants reported they had an education in, or worked in the field of computer science, computer engineering or information technology; 10.0% of participants reported that they were aware of a law in the U.S. that required companies to provide a "do not sell" option and explicitly mentioned the CCPA or California when asked to name or describe the law.

2.3 Data Analysis

Similar to our previous studies [1,2], we followed a systematic qualitative data analysis approach to categorize all open-ended responses provided by participants.⁶ For likert questions regarding attention, intention to click, and expectations about specific scenarios, we ran binomial regression models on a binary variable of *likely* (including "definitely" and "probably") versus *unlikely* (including "not sure," "probably not," and "definitely not"), with the five icon conditions as the key independent variable and participants' demographics (age, gender, race, region within California, education, and technical background) as control variables. To ensure the regression models fit, we binned some demographic variables into fewer categories (e.g., for age we binned the original seven categories into three: "18 to 34 years," "35 to 54 years," and "55 years and over"). We also excluded categories with too few instances for all demographic variables (e.g., "other" and "prefer not to answer"). For ratings regarding each icon's ability to convey the "do-not-sell" concept, we conducted a Friedman test, followed by pairwise Wilcoxon signed rank test, to test whether rating distributions between different icon conditions were significantly different.

⁵ Detailed comparisons of the demographics of our study's participants vs. California's population are provided in Appendix B.

⁶ Our codebooks for qualitative analysis are included in Appendix C.

3. Results

We found that the presence of an icon attracted attention to the do-not-sell link, with *PriceTag* and *StopSign* performing better than others. The presence of an icon however does not aid participants in forming more correct expectations of what happens when the opt-out button is clicked, but might instead evoke partially correct expectations or even misconceptions. None of the icons was ranked by participants as conveying a do-not-sell choice particularly well. Participants exhibited a high intention to click on the icon/link. Their intention to click was primarily driven by curiosity, whereas reasons for not wanting to click the button were dominated by not being concerned about privacy or a lack of familiarity with the icon. Table 1 summarizes our quantitative findings for each condition.

3.1 Attention

To understand how well each icon stands out on a website, we (1) asked participants to find the “Delivery Information” link to subtly direct their attention to the bottom right of the page, (2) hid the screenshot and tested whether participants noticed and could recall the do-not-sell icon and link, and (3) showed the screenshot and asked participants the same question to see whether the icon stands out under deliberate attention. We next present our results in the same order.

3.1.1 Less than Half Could Accurately Recall Seeing the Do-Not-Sell Icon/Link

With the screenshot provided, 75.4% of participants were able to identify the delivery information link by mentioning the word “delivery” when describing the link, with no significant differences between conditions. This indicates that our task successfully got most participants to pay attention to the bottom right corner of the screenshot, thus ensuring that they had a fair chance of noticing the do-not-sell icon and link text two lines below, without being primed to look for it.

Without the screenshot provided, **only 40.6% of participants could accurately recall the do-not-sell icon and link text, with notable differences between conditions** (see Figure 3). Interestingly, even for those participants who successfully identified the delivery information link, only 41.1% of them could accurately recall the do-not-sell icon and link text. This suggests that the icon and link were not salient enough to be noticed and remembered by the majority of participants, even when users’ attention was deliberately directed to the nearby area of the web page.

Category	 DoNot	 Person	 PriceTag	 StopSign	None
Attention					
Successful recall	38%	40%	52% (** vs. None)	43% (* vs. None)	31%
Communication of “Do Not Sell”					
Likely: DNS confirmation (correct)	89%	89%	91%	89%	91%
Likely: DNS more info (correct)	79%	83%	87%	82%	86%
Likely: DNS choices (correct)	69%	66%	73% (** vs. Person)	67%	79% (* vs. Person)
Likely: privacy ads (incorrect)	33%	31%	23% (* vs. DoNot)	25%	25% (* vs. DoNot)
Likely: give selling permission (incorrect)	13%	13%	9%	12%	14%
Likely: receive unwanted emails (incorrect)	15%	12%	8%	12%	9%
Likely: payment options (incorrect)	14%	11%	6%	8%	8%
Likely: discounts (incorrect)	10%	6%	5%	7%	6%
Icon Preferences					
Mean score for conveying DNS choices (0 to 6, the higher the better)	2.41 (SD: 1.35)	2.27 (SD: 1.30)	1.60 (SD: 1.18)	1.81 (SD: 1.26)	N/A
Intention to Click					
Likely to click	65%	61%	66%	58%	60%

*Table 1: Comparison of icons based on quantitative data analysis. . * denotes significance for statistical tests (“*” means $p < 0.05$, “**” means $p < 0.01$, “***” means $p < 0.001$). Icon preferences: DoNot and Person significantly more preferred than other icons in pairwise comparisons.*

3.1.2 “PriceTag” and “StopSign” Performed the Best in Drawing Attention

The *PriceTag* icon performed the best in attracting participants’ attention, with a 52% successful recall rate, whereas the *None* (no icon) condition performed the worst with only a 31% successful recall rate. The follow-up regression analysis showed that participants who were assigned to the *PriceTag* or *StopSign* icon were significantly more likely to accurately recall the do-not-sell icon and link text than those who did not see an icon ($OR^7=2.10$, $p=0.002$; $OR=1.74$, $p=0.02$). Participants who saw the *DoNot* or *Person* icon were not significantly more likely to accurately recall the do-not-sell icon and link text than those who did not see an icon. We conclude that ***PriceTag* and *StopSign* icons stood out the most to participants and successfully increased attention to and recall of the icon and link text, while the other two icons did not.**

When the screenshot was visible, 90.2% of participants could accurately identify the do-not-sell icon and link text, with no significant differences between conditions. **This indicates that all candidate icons, as well as the link text without an icon, were easily located if participants deliberately looked for them.**

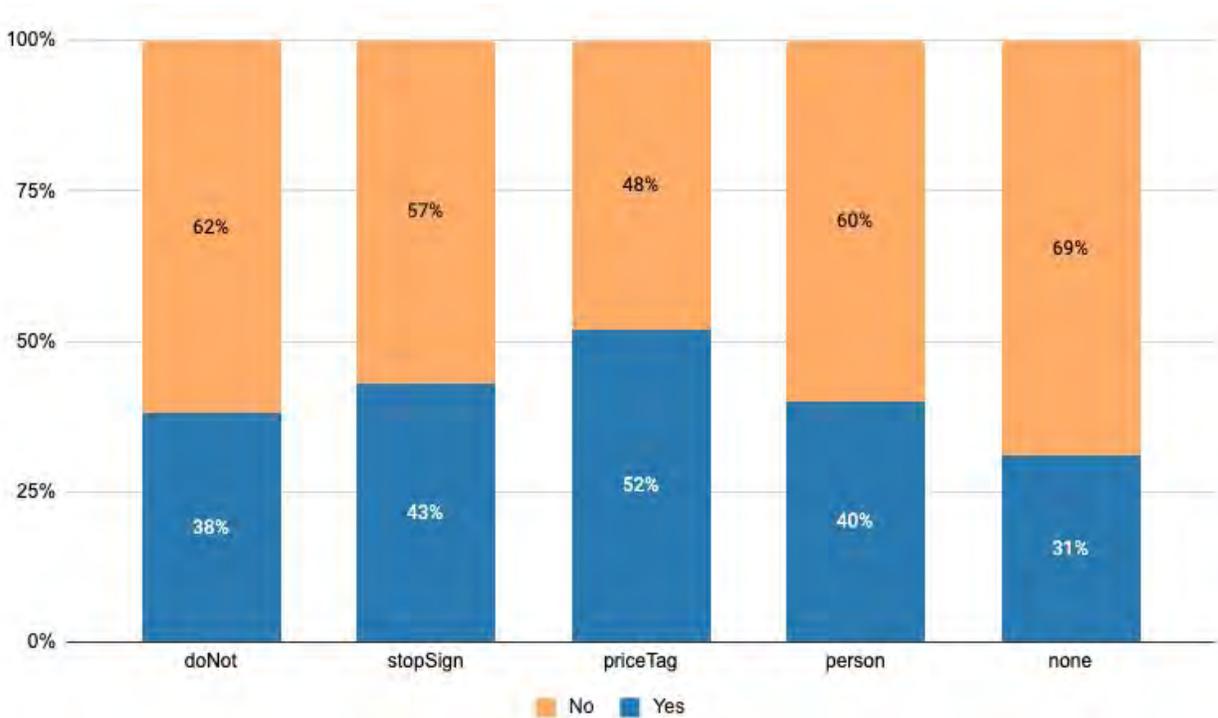


Figure 3: Percentage of participants who could accurately recall the do-not-sell icon and link without the screenshot in each icon condition.

⁷ “OR” stands for “odds ratio” — we used odds ratio as the effect size for all binomial regression analysis. $OR = 1.68$, 3.47 , and 6.71 are equivalent to Cohen's $d = 0.2$ (small), 0.5 (medium), and 0.8 (large) [9].

3.2 Communication of “Do Not Sell”

To understand how well each icon, when coupled with the link text, indicates the presence of choices related to “Do Not Sell My Personal Information,” we first asked participants to describe what they expected to happen if they clicked on the icon/link that they were shown. We then presented a set of scenarios and asked participants to rate how likely they expected each to happen after clicking the icon/link.

3.2.1 Correct Expectations Related to Do-Not-Sell Are Common

We grouped participants’ open-ended responses regarding what they expected to happen when clicking on the icon/link into three categories (correct, semi-correct, and incorrect) according to the possible interactions allowable under the CCPA. As seen in Figure 4, the distribution of responses was similar across the four conditions with an icon. Interestingly, only showing the link text without any icon resulted in notably more correct interpretations of what would happen after clicking the opt-out link (64%), i.e., those related to do-not-sell information and choices, and fewer partially correct interpretations (31%), i.e., privacy-related information, but not necessarily related to do-not-sell.

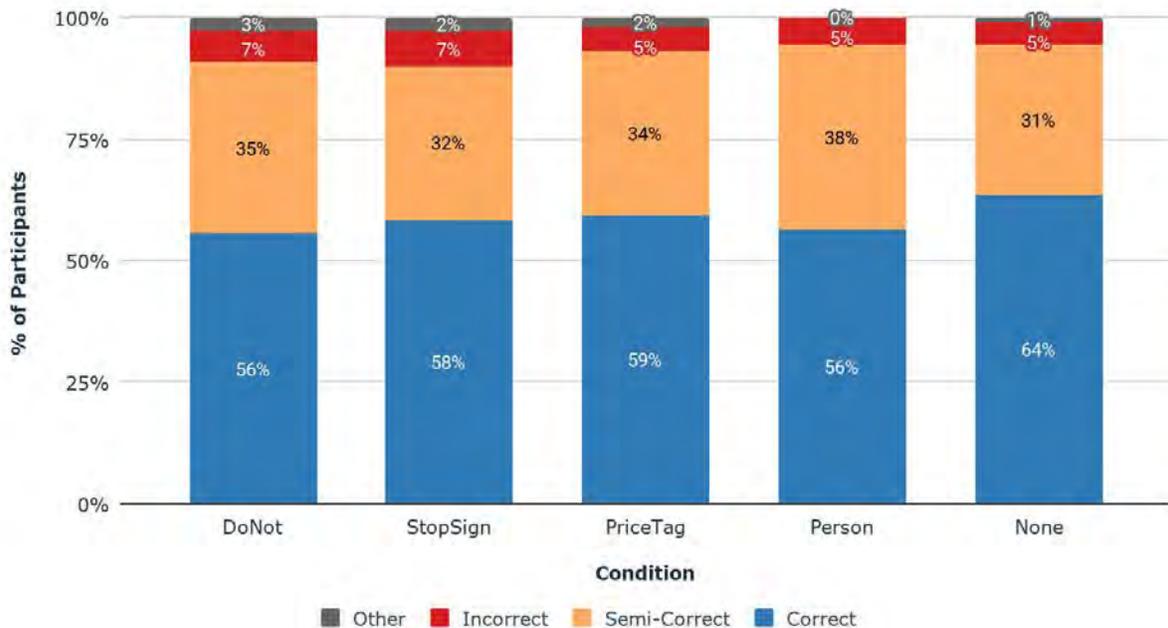


Figure 4: Distribution of participants’ responses to the question “What do you think would happen if you clicked on the symbol and link in the highlighted area on this web page?”⁸

⁸ Responses that contained multiple expectations are categorized under their “less correct” interpretation. Responses categorized as “other” were those that were not classified as correct/semi/incorrect, i.e., responses that do not fit into our existing codebook, as well as responses including nonsensical text.

Correct expectations: participants' most frequent expectations were consistent with the button's intention. The most common expectation, reported by 23% (236) of participants, was that clicking the icon/link would bring them to a page with options about the sale of their personal information or a page where they could submit a request that the company not sell their information. Eleven percent (112) of participants further specified that they would need to provide further information to the company or submit a form in order to make a do-not-sell request. Another common expectation, reported by 17% (172) of participants, was that they would see more information about the company's do-not-sell policy or instructions on how to exercise the option. Not as common, yet still a correct possible implementation of do-not-sell, was the expectation that the user would be brought to a page where they would have to confirm their do-not-sell request, mentioned by 4% (42) of participants.

Semi-correct expectations: participants also reported expectations that demonstrated an understanding that the do-not-sell icon/link was related to privacy, but did not correspond to the CCPA regulations' requirements for this opt-out button. A common semi-correct expectation was that clicking the icon/link would immediately apply the do-not-sell request, as described by 11% (109) of participants. Another 12% (122) of participants stated the link would bring them to the company's privacy policy or information about the company's data practices. A subset of 81 participants (8%) thought the link would lead to information about privacy choices, or increase the level of privacy protection on the website in some way.

Incorrect expectations: much less frequently, participants' responses highlight misconceptions related to the do-not-sell choice. Twenty-three participants thought that the icon/link was a scam or would direct them to a malicious website. Another fourteen participants described that clicking the icon/link would lead to less privacy protection, such as enabling the website to sell their data. Eight participants expected to be brought to a page where they would have to pay in order to make a do-not-sell request to the company. Ten participants expressed doubt that the company would honor a do-not sell request, or thought that the company would make exercising such a choice excessively cumbersome.

The findings above were further corroborated by the likelihood ratings for the eight given scenarios. As seen in Figure 5, the three scenarios about correct expectations related to do-not-sell (seeing more information, making choices, or confirming a do-not-sell requests) were considered likely (including "probably" and "definitely") to happen by over 70% of participants, whereas the other five incorrect scenarios were not considered likely by very many participants. Notably, the expectation of being taken to a page "with ads about privacy and security products" was higher than the other incorrect scenarios, with 27% of participants stating it would "probably" or "definitely" happen.

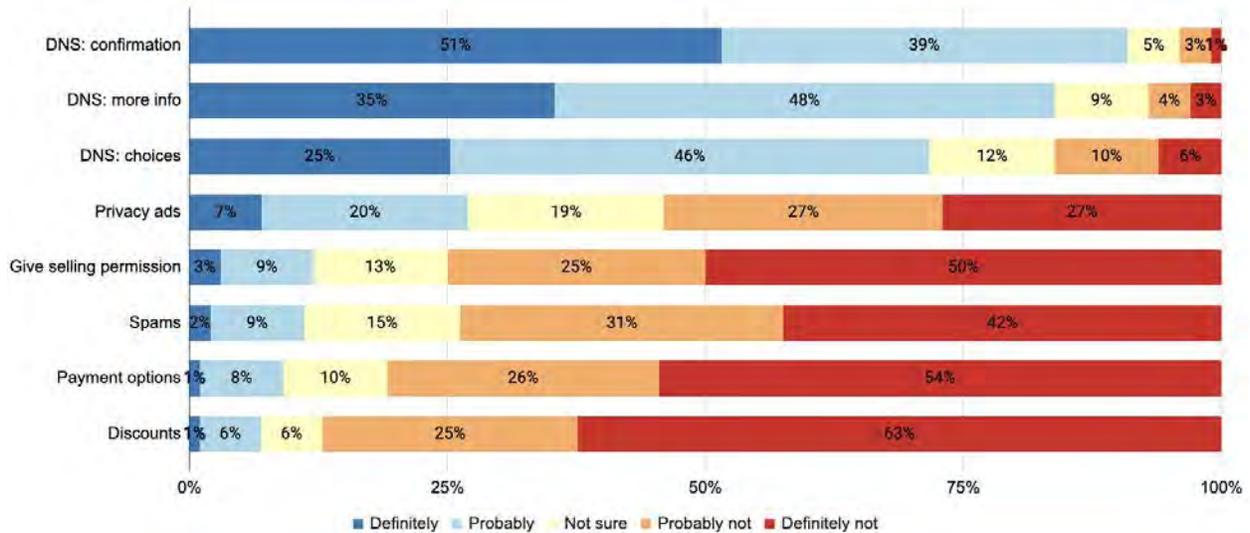


Figure 5: Distribution of participants' responses to the question "Which of the following do you think could happen if you clicked on this icon and link?" for eight provided scenarios.

3.2.2 No Icon Performed Best in Creating the Expectation of Do-Not-Sell Choices

Our regression models on participants' rated likelihood for the eight given scenarios revealed significant differences between icon conditions for three scenarios. For the scenario "It will take me to a page with choices about how my personal information is sold by the website," which is the most ideal scenario and closely aligns with the CCPA's requirement, between 66-79% participants across the five conditions considered this would "probably" or "definitely" happen (see Figure 6). **Only displaying the link text (no icon), performed best, with notable advantages over conditions with an icon.** The regression analysis further showed that *no icon* and *PriceTag* were significantly more effective at creating the expectation of do-not-sell choices than *Person* (OR=1.89, p=0.01; OR=1.95, p=0.008).

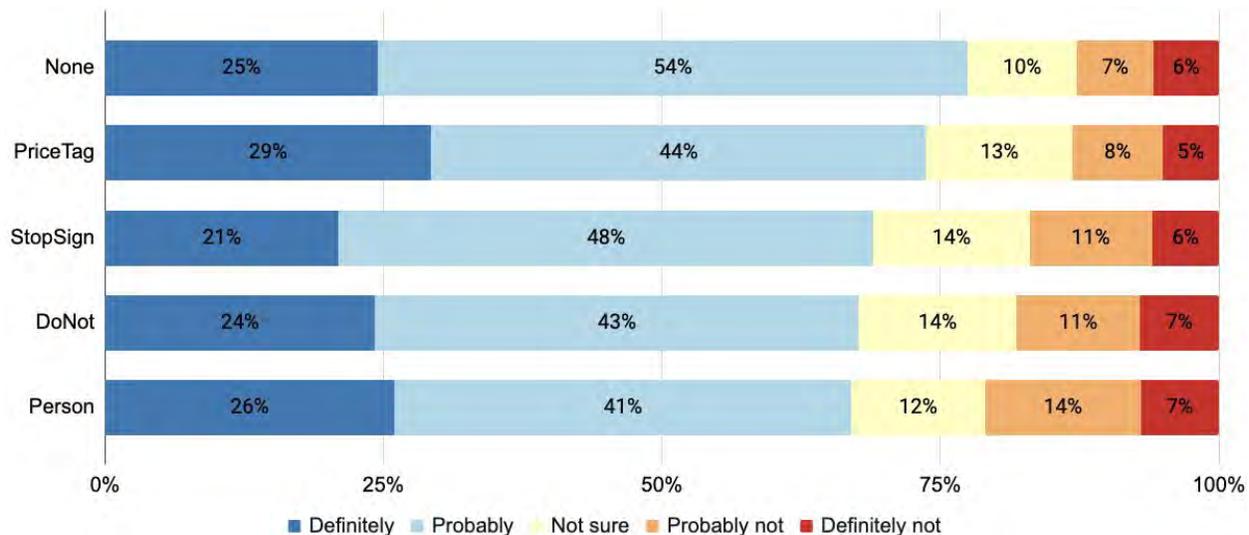


Figure 6: Distribution of participants' rated likelihood for the scenario "It will take me to a page with choices about how my personal information is sold by the website."

3.2.3 Potential Misconceptions Generated By Icons

For most of the incorrect scenarios, we found the choice of the icon, or even having an icon, had minimal impact on participants' expectations. However, it is worth noting that **for the DoNot icon, one misconception — ads about privacy and security products — was significantly more common than for other icons.** Specifically, 33% of participants who saw the DoNot icon expected that they would be redirected to privacy and security products ads. The likelihood of DoNot generating such misconception was significantly higher than for PriceTag (OR=1.71, p=0.03) and no icon (OR=1.81, p=0.02). Based on these findings, we concluded that **the DoNot icon should be avoided if the goal is to reduce misconceptions about privacy and security ads.**

3.3 Icon Preferences

After answering questions pertaining to the particular icon (or no icon) to which participants were assigned, we showed participants all four candidate icons in randomized order and asked them to rate how well each icon conveyed the concept of "Do Not Sell My Personal Information," to provide an opportunity for elaborating opinions and drawing comparisons between icons.

3.3.1 "DoNot" and "Person" Favored for Conveying "Do-Not-Sell" Concept

Our previous analysis of the scenarios show that all candidate icons, coupled with the link text, generated correct expectations about possible outcomes under the CCPA. Nevertheless, **none of the candidate icons received mean ratings that reached the "moderately" level for conveying the concept of "Do Not Sell My Personal Information," i.e., participants**

thought these icons did not represent this concept well.⁹ Between the four icons, *DoNot* and *Person* performed better than the other two icons (see Figure 7). A Friedman test (non-parametric ANOVA) on the provided ratings, after excluding responses that selected “I don’t know,” further confirmed the statistically significant differences of rating distributions between icon conditions, $X^2(3)=437.2$, $p<0.001$, with a small effect size detected, Kendall’s $W=0.16$. Pairwise Wilcoxon signed rank test between groups, with Bonferroni correction applied, revealed statistically significant differences between all pairs of conditions ($p<0.001$) for all comparisons, except *DoNot* vs. *Person*.

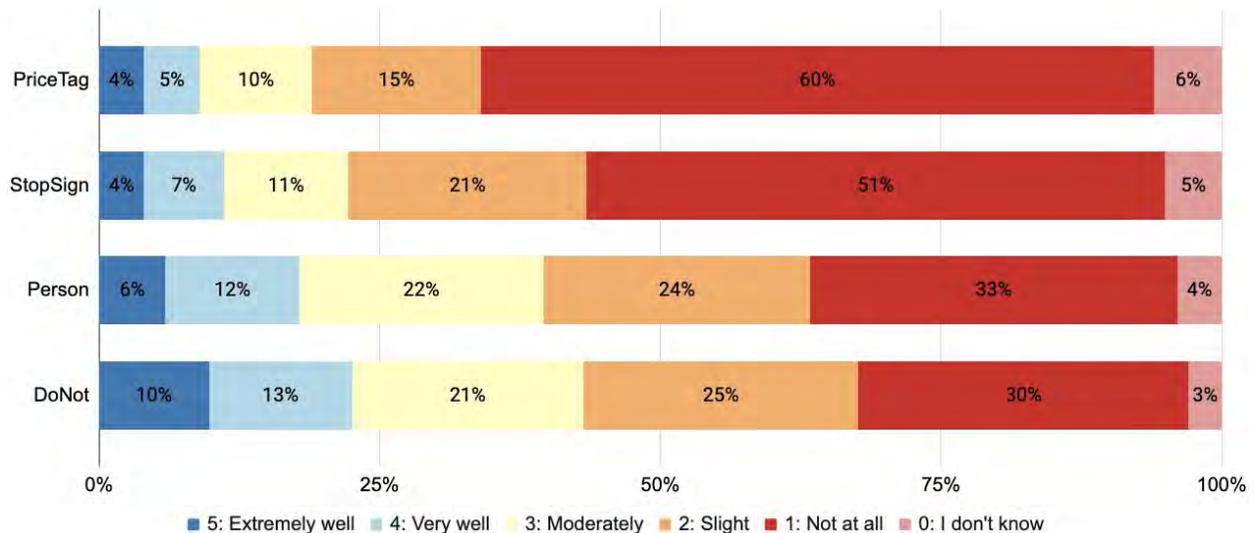


Figure 7: Distribution of participants’ responses for each icon to “How well does the icon convey that there is an option to tell a website “do not sell my personal information?”

3.3.2 All Icons Conveyed Inaccurate Information When Viewed Alone

As shown in Table 2, our analysis of participants’ open-ended responses about the reasons behind their ratings suggests that **all icons frequently conveyed information other than “do not sell my personal information.”** The interpretation of things other than “Do Not Sell” occurred most frequently with the *PriceTag* icon (87.3%), followed by *StopSign* (82%), *Person* (67%), and *DoNot* (64.2%). Table 3 shows examples of some of the most common icon interpretations.

Conversely, a small percentage of participants expressed a positive opinion about the icon (“meaningful icon”), saying that the icon is clear / straightforward, or gave interpretations that reflect they had a correct understanding of the concept the icon intended to convey (e.g., “It says my information will not be sold for a dollar amount”). This occurred mostly with participants who saw the *DoNot* icon (29.4%), followed by *Person* (28.1%), *StopSign* (11.7%), and *PriceTag* (9%). Fewer participants explicitly stated that the icon conveyed the concept of “do not,” “stop,”

⁹ The mean and standard deviation (SD) for each icon’s received ratings: *DoNot* (mean=2.41, SD=1.35); *Person* (mean=2.27, SD=1.30); *PriceTag* (mean=1.60, SD=1.18); *StopSign* (mean=1.81, SD=1.26).

or “prohibit” and most of them said this for the *DoNot* icon. Few participants mentioned that any of the icons except the *Person* icon conveyed anything related to personal information.

Theme	Code								
		DoNot		StopSign		PriceTag		Person	
Conveying intended meaning	Meaningful icon	249	25.1%	99	11.2%	76	8.4%	129	13.0%
	Conveyed: do not	42	4.2%	2	0.2%	3	0.3%	16	1.6%
	Conveyed: personal info	0	0.0%	2	0.2%	2	0.2%	133	13.4%
Not conveying intended meaning	Convey inaccurate information	197	19.9%	280	31.7%	370	41.0%	162	16.3%
	Not conveyed: personal info	139	14.0%	122	13.8%	109	12.1%	102	10.3%
	Ambiguous	108	10.9%	161	18.2%	148	16.4%	79	8.0%
	Confusing	53	5.3%	40	4.5%	47	5.2%	106	10.7%
	Unclear	53	5.3%	43	4.9%	54	6.0%	96	9.7%
	Icon not sufficient	40	4.0%	26	2.9%	16	1.8%	55	5.5%
	Loose connection with privacy	25	2.5%	13	1.5%	15	1.7%	10	1.0%
	Prior knowledge needed	19	1.9%	9	1.0%	8	0.9%	20	2.0%
	Not conveyed: do not	2	0.2%	27	3.1%	17	1.9%	34	3.4%
	Not conveyed: choices	0	0.0%	3	0.3%	3	0.3%	0	0.0%
Not related to icon meaning	Icon stands out	28	2.8%	36	4.1%	22	2.4%	18	1.8%
	Other	16	1.6%	0	0.0%	0	0.0%	2	0.2%
	Icon is simple	7	0.7%	3	0.3%	1	0.1%	1	0.1%
	Icon too small	5	0.5%	5	0.6%	2	0.2%	10	1.0%
	Icon does not stand out	5	0.5%	12	1.4%	6	0.7%	8	0.8%
	Complicated	3	0.3%	0	0.0%	3	0.3%	10	1.0%

Table 2: Summary of explanations of ratings for how well each icon conveyed the concept of “Do Not Sell My Personal Information. Note, some participants provided multiple explanations.

Icon	Common interpretations of icon meaning other than “Do Not Sell”
 <i>DoNot</i>	<ul style="list-style-type: none"> • [Sales related, 110] “Make me think of sales or buying something” / “Indicate free offers or information” • [Money related, 117] “A sign for no money” / “I can only think of no money/no cost” • [Payment related, 50] “You can’t pay with cash” / “An icon that would be used to stop payment”
 <i>StopSign</i>	<ul style="list-style-type: none"> • [Money related, 125] “Something about spending money” / “This indicates money and nothing else” • [Sales related, 78] “Sales prices and discounts related to the products” / “It almost looks like a discount sign” • [Payment related, 54] “The number of payment options accepted” / “Stopping some type of payment transaction”
 <i>PriceTag</i>	<ul style="list-style-type: none"> • [Sales related, 339] “The price or the discount of something” / “Something is for sale” • [Shopping related, 30] “Something is being bought” / “It could be a icon for purchasing a product” • [Money related, 14] “How to stop paying money” / “it’s saying stop spending money.”
 <i>Person</i>	<ul style="list-style-type: none"> • [Money related, 43] “Currency exchange” / “The person is receiving money” • [Payment related, 40] “A payment option of some kind” / “The checkout area where I can finish my purchases” • [Sales related, 31] “A common symbol meaning the store is having a sale” / “A link to earn extra money or for discounts”

Table 3: Common interpretations of icon meaning other than “Do Not Sell” for candidate icons and their frequency.

3.3.3 Most Icons Failed to Convey the Concept of Personal Information

A notable number of participants mentioned that they were not able to connect the icon with the concept of personal information. This is especially the case for *DoNot*, *PriceTag*, and *StopSign*. For *DoNot*, 14.0% of participants commented that even though the meaning of the icon was somewhat clear, the icon did not contain any element that indicated the involvement of personal information. For *StopSign*, 13.8% of participants noted the same point, possibly because the stop sign-shaped icon and the dollar sign made it look more like stopping a “money-related” matter, not necessarily personal information. For *PriceTag*, 12.1% of participants did not infer the relationship between the icon and personal information, and commented that the icon conveyed a stronger sense of “sales” rather than “personal information.” While 10.3% of participants also failed to derive the sense of personal information from *Person*, 13.5% found the opposite, commenting that the person icon in combination with the dollar sign reflected the sense of selling something personal for money.

3.3.4 Icons Only Make Sense When Accompanied by the Link Text

Similar to our previous studies [1,2], 137 participants indicated that the icons themselves were not sufficient and would only make sense when accompanied by the link text. This could possibly be due to our finding, reported above, that all icons except *Person* do not have a specific design element that conveyed to participants a sense of personal information. For instance, a participant wrote: “Not reading the text and just seeing the image, it’s not very clear. Stop sign + money, nothing in it inherently signifies personal information.” Other participants commented that text is needed because the icon only conveys a too vague concept of money, sales, or payment - e.g., “The icon communicates nothing at all without the accompanying text, other than it’s something related to money which could be a million things.”

Relatedly, 66 participants noted that they could not make sense of the icon because the icon was fairly new to them, e.g., “If I saw that icon without knowing what it was I would not know what it meant.” Sometimes prior knowledge is also needed to understand certain elements of the icon in order to derive its meaning (“This might make sense for folks who know what a stop sign is”), which could create problems in a cross-cultural context (“The stop sign works in America anyway, because it says STOP”). Other participants noted that there would always be a learning curve for new icons (“Unless it becomes a world wide web known symbol like a lock means the website is secure, it could be loosely translated to mean anything the site wants it to be”), and emphasized on the importance of public education (“More consumer education is needed before this icon is widely adopted”). These comments echo our previous recommendations [1,2] that during an icon’s initial adoption stage, an icon should always be used in combination with the link text until people are familiar with it.

3.4 Intention to Click

We asked participants how likely they were to click on the icon and link text if they noticed them for the first time on a website. This was followed by an open-ended question that asked them to elaborate on the rationale behind their selected answer option.

3.4.1 Participants Exhibited High Intentions to Click

Between 58-66% participants across the five conditions reported they would “definitely” or “probably” click on the icon and link text when first noticing them on a website. This indicates that all candidate icons, as well as the link text text alone, were sufficient to motivate users to take action or click if they have attracted the user’s attention. Our regression analysis showed no statistically significant differences in intention to click between any two conditions, indicating that **the choice of the icon, or even having an icon, had minimal impact on participants’ intention to click on the icon/link text for further interactions.**

3.4.2 Top Reasons for Intending to Click

We report top reasons for intending or not intending to click the button for all conditions together, since our analysis shows that these reasons were consistent across conditions. For participants who reported they would “definitely” or “probably” click on the icon and link text, **the most common reason, mentioned by 254 (26.1%) participants, was that they wanting to click the icon/link was motivated by curiosity.** Among them, 102 mentioned their curiosity on a generic level without specifying the subject matter. 106 reported being curious to learn about the website’s data practices, such as how the website sold or did not sell their data, or whether their data was safe and secure. 46 explicitly mentioned that they were curious about what options were available for “Do Not Sell My Personal Info.”

Aside from curiosity, 142 (14.6%) participants indicated that their intention to click was rooted in the opposition to the idea that companies could make profits by selling consumers’ data. 96 (9.9%) participants mentioned that they valued their privacy online by saying “my personal information is everything” or “I always worry about my personal information.” They further listed several potential consequences if their privacy was invaded, such as “a lot of spam” or “identify theft.” As such, they were motivated to explore options that could protect their privacy.

3.4.3 Top Reasons for Intending not to Click

For participants who reported they would “definitely not” or “probably not” click on the icon and link text or that they were not sure,¹⁰ the top reason for not clicking was that they had “no concerns,” mentioned by 93 (9.6%) participants. Among them, 60 specifically mentioned that they had no concerns over their personal information, out of the notion that their personal information would be collected and sold regardless and there was nothing they could do to prevent that from happening. The other 33 participants noted that they generally did not care about their own privacy.

Additionally, 66 participants indicated that they were not motivated to click because the icon was unfamiliar/appeared fairly new to them, and there was no way for them to figure out its legitimacy. 42 participants mentioned that they would not click due to personal habits, e.g., they tended to skip links and pages that were not related to their primary purposes of visiting the website. 52 participants were unsure whether they would click, since the action would largely depend on what they would do on the website: if they were only browsing the website, they might not click; once they decided to make a purchase, they would potentially click the icon and explore options to protect their personal information.

¹⁰ We treated “not sure” as not having the intention to click, as our data shows that when participants selected this answer option, their open-ended responses tended to explain why they would not click the icon.

3.6 Recognizability at a Small Scale

In the course of working with the candidate icons, we observed that most of them were difficult to recognize when scaled to a small size (e.g., 16x16 pixels). The fine lines in PriceTag and Person could be particularly problematic, while StopSign was easier to interpret when scaled down.

3.5 Comparison with Previous Findings

In the current study we did not ask participants to comment on what they thought the icons conveyed until after they had seen them with the accompanying text. However, in our February 4 report [1] (which surveyed participants from across the US, not just California), we reported on participants' responses when we asked each of them to interpret one of five proposed icons without any accompanying text in our round 2 icon test (four icons developed by us; one proposed by the DAA). Three of those icons are similar to three of the icons tested in the current study, and thus it is useful to revisit our previous findings. In particular, the *Person* icon resembles the previously tested *ID card* icon, the *DoNot* icon resembles the previously tested *Slash-dollar* icon, and the *StopSign* icon resembles the previously tested *Stop-dollar* icon.

As shown in the summary of responses from the February 4 report shown in Table 4, most participants who saw these icons had misconceptions about the meaning of each icon, and these misconceptions were similar to what we found in the current study when we asked participants to explain the reason behind their ratings for each icon (summarized in Table 3).

The presence of the dollar sign in three of the icons invoked the concept of money. In the case of the *ID card* it most commonly conveyed the incorrect idea that something costs money, and only occasionally the correct (but incomplete) notion that the symbol was related somehow to a person and money. In the case of the *Slash-dollar* icon, it mostly conveyed that something is free or that cash/dollars are not accepted, and only occasionally conveyed the correct (but incomplete) notion that selling is not allowed. In the case of the *Stop-dollar* icon, it mostly conveyed concepts related to money and prices, with no correct interpretations. The *DAA* icon did not fare any better, with most participants interpreting it as conveying concepts related to getting more information or as an audio/video play button.

On the other hand, our stylized *Toggle* icon was correctly interpreted by most participants as conveying concepts related to accepting/declining or activating/deactivating, or more generally, concepts related to options, choices, or settings. This is also incomplete, as it does not convey the kind of options that can be exercised. However, unlike the other icons tested, the *Toggle* icon did not tend to mislead participants. By reliably conveying “choice,” this icon could complement and emphasize the “Do Not Sell” tagline and its correct interpretation, which was one of the reasons we recommended it.

Icon From Previous Round 2 Icon Test	Similar Icon From Phase 2 Study	Common Interpretations (# of participants) From Previous Round 2 Icon Test
Toggle 		<ul style="list-style-type: none"> ● accept/decline something (11) ● activate/deactivate something (5) ● okay/exit options (4) ● mark as true/false (4)
DAA 		<ul style="list-style-type: none"> ● get more information (15) ● start audio/video content (7) ● denotes website is safe or private (3) ● move forward or next (2) ● something related to ads (1)
ID card 	Person 	<ul style="list-style-type: none"> ● something costs money (10) ● sending money to someone (4) ● account balance related (4) ● payment methods accepted by website (2) ● something related to a person and money (3) ● price related (2) ● receiving money from someone (2)
Slash-dollar 	DoNot 	<ul style="list-style-type: none"> ● something is free or requires no money (12) ● cash/dollars not accepted (7) ● money (4) ● selling is not allowed (1)
Stop-dollar 	StopSign 	<ul style="list-style-type: none"> ● money (14) ● price related (6) ● stop spending money (5) ● something costs money (2) ● stop (2)

Table 4: Summary of responses to “What does this symbol communicate to you?” from participants who saw icons without taglines in the Round 2 icon test reported in our prior study [1]. Correct interpretations are highlighted with bold text. Similar icons in our current study are shown in the second column.

The February 4 report also reported on the results of our Opt-Out Icon + Tagline Combination Study, in which we showed participants icon and tagline combinations in the context of the fictitious shoe retailer website and asked “What do you think would happen if you clicked on the symbol and link in the highlighted area on this web page?” We tested the *DAA icon*, *Slash-dollar icon*, *Toggle icon*, and no icon in combination with five taglines and no tagline. We revisited the results for these icons in combination with the “Do Not Sell My Personal Information” tagline. We found similar rates of correct responses for each of these icons. Among incorrect responses,

besides the misconceptions mentioned in Table 4 regarding what the symbol communicates, we found a small number of other types of misconceptions about what happens when the symbol/link is clicked, including that clicking on the *Toggle icon* might immediately cause the website to either start or stop selling personal information. These misconceptions occurred less frequently when the icon was paired with the “Privacy Options” tagline.

4. Conclusions

As can be seen from the summary of key findings from our quantitative analysis in Table 1, the effect of having an icon vs. no icon is nuanced. **While having an icon next to the link could make the link stand out (especially for the two octagon-shaped icons *PriceTag* and *StopSign*), more importantly, the tested candidate icons also negatively impacted participants’ ability to generate correct expectations related to do-not-sell, and might induce misconceptions.** In addition, all of the candidate icons received low average ratings between 1 (slightly) and 3 (moderately) on a 5-point scale in response to the question “How well does the icon convey that there is an option to tell a website ‘do not sell my personal information?’”

The *DoNot* icon was most preferred by participants, but still scored only 2.41 on the 1-to-5 preference scale. While 291 participants noted that it was meaningful or conveyed relevant concepts, 636 participants did not find it meaningful or stated that it conveyed concepts related to sales, money, or payments. It was also the icon most likely to convey incorrectly that clicking would lead to a page with ads about privacy and security products. It did not grab participants’ attention significantly more than a link with no icon.

The *Person* icon was the second most preferred by participants, but scored only 2.37 on the 1-to-5 preference scale. While 278 participants noted that it was meaningful or conveyed relevant concepts, 664 participants did not find it meaningful or stated that it conveyed concepts related to sales, money, or payments. It was also the icon least likely to convey that clicking would lead to a page with choices about how personal information is sold by the website. It did not grab participants’ attention significantly more than a link with no icon.

The *PriceTag* icon was most likely to grab participants’ attention. It was also the icon most likely to convey correctly that clicking would lead to a page with choices about how personal information is sold by the website and least likely to convey incorrectly that clicking would lead to a page with ads about privacy and security products. However, it was least preferred by participants, scoring only 1.60 on the 1-to-5 preference scale and it was the icon participants described most frequently as not conveying its intended meaning. While 81 participants noted that it was meaningful or conveyed relevant concepts, 787 participants did not find it meaningful or stated that it conveyed concepts related to sales, money, or shopping. In particular, 370 (41%) participants considered the icon as conveying inaccurate information.

The *StopSign* icon was second most likely to grab participants' attention. However, it was ranked third by participants, scoring only 1.81 on the 1-to-5 preference scale. While 103 participants noted that it was meaningful or conveyed relevant concepts, 724 participants did not find it meaningful or stated that it conveyed concepts related to sales, money, or payments. This icon appears to us to be the icon most recognizable at a small scale, but we did not test this with participants.

We found the same types of misconceptions about the meaning of icons when we tested similar designs for our February 4 report. However, as noted in Section 3.6, we also found that our previously tested stylized blue toggle icon reliably conveyed the concept of choice, and thus might be worth considering as an alternative.

We recommend refraining from using one of the four tested icons to avoid generating problematic misconceptions. Instead, alternative icons should be considered and evaluated, or only the link text should be used, accompanied by clear stipulations in the CCPA regulations to mandate where the link should be placed. These measures should be accompanied by extensive public education efforts to increase consumers' awareness of the link and where it is commonly located.

References

1. L.F. Cranor, H. Habib, Y. Zou, A. Acquisti, J. Reidenberg, N. Sadeh, F. Schaub. Design and Evaluation of a Usable Icon and link text to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA. February 4, 2020.
<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-cranor.pdf>
2. L.F. Cranor, H. Habib, Y. Zou, A. Acquisti, J. Reidenberg, N. Sadeh, F. Schaub. User Testing of the Proposed CCPA Do-Not-Sell Icon. February 24, 2020. In *Written Comments Received During 2nd 15-Day Comment Period*,
<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-2nd-15day-comments-031120.pdf>
3. Revised Proposed Regulations, modified February 10, 2020. Office of the California Attorney General.
<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf>
4. Revised Proposed Regulations, modified March 11, 2020. Office of the California Attorney General.
<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-clean-031120.pdf>
5. Redmiles, Elissa M., Sean Kross, and Michelle L. Mazurek. "How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples." In 2019 IEEE Symposium on Security and Privacy (SP), pp. 1326-1343. IEEE, 2019.

6. United States Census Bureau. 2020. 2018 American Community Survey 1-Year Estimates Data Profiles: ACS Demographic and Housing Estimates (California). <https://data.census.gov/cedsci/table?hidePreview=true&q=DP05%3A%20SELECTED%20HOUSING%20CHARACTERISTICS%20IN%20THE%20UNITED%20STATES&table=DP05&tid=ACSDP1Y2018.DP05&lastDisplayedRow=29&g=0400000US06>
7. United States Census Bureau. 2020. 2018 American Community Survey 1-Year Estimates Data Profiles: Selected Social Characteristics in the United States (California). <https://data.census.gov/cedsci/table?hidePreview=true&q=DP02%3A%20SELECTED%20SOCIAL%20CHARACTERISTICS%20IN%20THE%20UNITED%20STATES&table=DP02&tid=ACSDP1Y2018.DP02&lastDisplayedRow=29&g=0400000US06>
8. United States Census Bureau. 2020. Annual Estimates of the Resident Population for Counties: April 1, 2010 to July 1, 2019 (California). <https://www2.census.gov/programs-surveys/popest/tables/2010-2019/counties/totals/co-est2019-annres-06.xlsx>
9. Chen, H., Cohen, P., & Chen, S. (2010). How big is a big odds ratio? Interpreting the magnitudes of odds ratios in epidemiological studies. *Communications in Statistics—simulation and Computation*, 39(4), 860-864.

Appendix A: Survey Questions

Survey instruction

We will show you a screenshot of a website on the next page and will ask you to answer a number of questions about it. Make sure not to reveal any private or personally identifiable information about yourself or others in your responses to any open-ended questions.

Attention

[Display the screenshot]

Imagine you were shopping at this online store and you wanted to know whether you could have a pair of shoes shipped to you overnight. Do you see a link you could click to find out? If the text in the screenshot above is too small to read, please zoom in as needed.

- Yes
- No

[If “Yes” to the last question] Please describe the text of the link that could help you determine whether you could have a pair of shoes shipped to you overnight. *[Open-ended response]*

[Hide the screenshot]

Imagine you were shopping at this online store, and you were concerned about the store selling your personal information. Do you remember seeing any feature in the screenshot that you could use to prevent this from happening?

- Yes
- No

[If “Yes” to the last question] You saw a feature that you could use to prevent the store from selling your personal information. Please describe what the feature looks like. *[Open-ended response]*

[Display the screenshot]

Here is the same screenshot we showed you previously. Please take a look at it again. Do you see any feature in the screenshot that you could use to prevent the store from selling your personal information?

- Yes
- No

[If “Yes” to the last question] You saw a feature that you could use to prevent the store from selling your personal information. Please describe what the feature looks like. [Open-ended response]

Intention to click

[Display the screenshot, with icon and link highlighted in an orange box]

[Display the zoomed-in icon and link]

Imagine this was the first time that you noticed this icon and link text on this or any other website. Do you think you would click on the icon and link?

- Definitely not
- Probably not
- Not sure
- Probably
- Definitely

You indicated you would *[piped answer option from the last question]* click on the icon and link, if you noticed them for the first time on this or any other website. Please describe why you selected this answer option. *[Open-ended response]*

Communication of “Do Not Sell”

[Display the screenshot, with icon and link highlighted in an orange box]

[Display the zoomed-in icon and link]

What do you think would happen if you clicked on this icon and link? *[Open-ended response]*

Which of the following do you think could happen if you clicked on this icon and link? *[Answer options: definitely, probably, not sure, probably not, definitely not.]*

- It will take me to a page where I can confirm that I do not want my personal information to be sold by the website
- It will take me to a page with choices about how my personal information is sold by the website
- It will take me to a page with more details about how the website uses and shares my personal information
- It will give the website permission to sell my personal information
- It will cause the website to send me unwanted emails
- It will take me to a page with ads about privacy and security products
- It will take me to a page with sales, discounts, or free stuff
- It will take me to a page related to payment options

Icon preferences

[For each of the four icons, display the following two questions. The order of icons are randomized.]

How well does the following icon convey that **there is an option to tell a website "do not sell my personal information?"** *[Answer options: I don't know, not at all, slightly, moderately, very well, extremely well]*

Please explain why you gave this rating. *[Open-ended response]*

Familiarity with CCPA

Are you aware of any laws in the United States that require companies to provide a "do not sell my personal information" option?

- No
- Yes (please name or describe them): _____

Demographics

What is your age?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65-74
- 75-84
- 85 or older
- Prefer not to answer

What is your gender?

- Woman
- Man
- Non-binary
- Prefer to self describe: _____
- Prefer not to answer

What is your race / ethnicity? Please choose all that apply.

- White
- Black or African American
- Hispanic or Latino

- American Indian or Alaska Native
- Asian
- Native Hawaiian or other Pacific Islander
- Other: ____
- Prefer not to answer

What is the highest level of education you have completed?

- Less than high school
- High school degree or equivalent
- Some college, no degree
- Associate's degree, occupational
- Associate's degree, academic
- Bachelor's degree
- Master's degree
- Professional degree (e.g., J.D. and M.D.)
- Doctoral degree
- Prefer not to answer

What was your total household income before taxes during the past 12 months?

- Under \$15,000
- \$15,000 to \$24,999
- \$25,000 to \$34,999
- \$35,000 to \$49,999
- \$50,000 to \$74,999
- \$75,000 to \$99,999
- \$100,000 to \$149,999
- \$150,000 or above
- Prefer not to answer

In which state do you currently reside? *[A drop down list of the 50 states, D.C. and Puerto Rico, in addition to "I do not reside in the United States" and "Prefer not to answer"]*

[If "California" is selected] Please enter the 5-digit ZIP code of the area you currently reside in. If you prefer not to answer, please enter "00000".

[If "California" is selected] In which county of California do you currently reside? *[A drop down list of all California counties, in addition to "I don't know" and "Prefer not to answer"]*

Which of the following best describes your primary occupation?

- Administrative support (e.g., secretary, assistant)
- Art, Writing, or Journalism (e.g., author, reporter, sculptor)
- Business, Management, or Financial (e.g., manager, accountant, banker)
- Education or science (e.g., teacher, professor, scientist)

- Legal (e.g., lawyer, paralegal)
- Medical (e.g., doctor, nurse, dentist)
- Computer Engineering or IT Professional (e.g., programmer, IT consultant)
- Engineer in other fields (e.g., civil or bio engineer)
- Service (e.g., retail clerk, server)
- Skilled Labor (e.g., electrician, plumber, carpenter)
- Unemployed
- Retired
- College student
- Graduate student
- Mechanical Turk worker
- Other: ____
- Prefer not to answer

Which of the following best describes your educational background or job field?

- I have an education in, or work in, the field of computer science, computer engineering, or IT
- I do not have an education in, nor do I work in, the field of computer science, computer engineering or IT
- Prefer not to answer

Appendix B: Participant Demographics

Category	Our Sample	Californians
<i>Gender</i>		
Men	50.4%	49.7%
Women	47.6%	50.3%
Non-binary	1.3%	N/A
Prefer not to answer	0.7%	N/A
<i>Age</i>		
18 to 24 years	15.9%	8.5%
25 to 34 years	40.5%	15.3%
35 to 44 years	23.2%	13.3%
45 to 54 years	11.7%	12.8%
55 to 64 years	6.4%	12.1%
65 to 74 years	1.9%	8.3%
75 years and over	0.2%	6.0%
Prefer not to answer	0.2%	N/A
<i>Race</i>		
White	47.9%	72.1%
Black or African American	4.9%	6.5%
American Indian and Alaska Native	0.2%	1.6%
Asian	22.3%	15.3%
Native Hawaiian and other Pacific Islander	0.5%	0.5%
Hispanic or Latino	18.1%	39.3%
Two or more races	4.6%	36.8%

Other / Prefer not to answer	1.6%	N/A
------------------------------	------	-----

Education

Less than high school	0.3%	16.2%
-----------------------	------	-------

High school degree or equivalent	7.5%	20.7%
----------------------------------	------	-------

Some college, no degree	22.7%	20.8%
-------------------------	-------	-------

Associate's degree (academic or occupational)	10.3%	8.0%
---	-------	------

Bachelor's degree	45.5%	21.3%
-------------------	-------	-------

Graduate or professional degree	13.3%	12.9%
---------------------------------	-------	-------

Prefer not to answer	0.4%	N/A
----------------------	------	-----

Region within California

Bay Area	13.5%	19.0%
----------	-------	-------

Central	13.3%	11.0%
---------	-------	-------

Central Coast	3.5%	5.1%
---------------	------	------

Desert	10.8%	12.0%
--------	-------	-------

Northern California	10.7%	10.6%
---------------------	-------	-------

Southern	46.6%	42.3%
----------	-------	-------

Don't know / Prefer not to answer	1.6%	N/A
-----------------------------------	------	-----

Appendix C: Codebook

Open-ended responses for delivery link (i.e., responses to “Please describe the text of the link that could help you determine whether you could have a pair of shoes shipped to you overnight.”)

Code	Definition	Example
correct	The text mentions the word "delivery"	"delivery link" "delivery information"
incorrect	The text does not include words that are relevant to delivery	"find in the order list" "contact us" "shipping information"
n/a	Use it when the cell is empty	

Open-ended responses for do-not-sell icon/link (i.e., responses to “You saw a feature that you could use to prevent the store from selling your personal information. Please describe what the feature looks like.”)

Code	Definition	Example
correct	The text mentions either a (red) icon or the link text by naming it (do not sell my personal information or do not sell my info), or both, or the location (e.g., the bottom right of the page)	"It was a red icon and it stated next to it: Do not sell my personal information"
incorrect	The text mentions something vague about privacy/security, but does not call out the do-not-sell icon or link	"privacy concerns related" "There was a link about privacy" "privacy and security"
n/a	Use it when the cell is empty	

Open-ended responses for CCPA description (i.e., responses to “Are you aware of any laws in the United States that require companies to provide a “do not sell my personal information” option? If yes, please name and describe them.”)

Code	Definition	Example
correct	The text spells out CCPA (California Consumer Protection Act) or mentions California specifically	"California law requires all websites that sell personal information to offer an opt out option."
incorrect	The text mentions "a federal law" or some other laws that are unrelated to	"I don't know what the laws are called, but I do believe there are Federal laws

do-not-sell

that protect us from having our personal information sold."

n/a

Use it when the cell is empty

Open-ended responses for expectations (i.e., responses to "What do you think would happen if you clicked on this icon and link?")

Code	Definition	Example
do not sell: choices	Specific mentioning that consumers will have the option to choose whether or what types of data can or cannot be sold to third-parties by the site	It would give me a bunch of options on not to sell my information.
do not sell: confirmation	The link will lead to a page that double checks the user does not want their information to be sold	I would be taken to a page where I am given more information about how this store handles my data and asked to make a final confirmation of my choice.
do not sell: immediate	The company will stop selling the user's personal data immediately	Exactly what it says. Would just not put me on whatever lists that get sold to third parties.
do not sell: more info	More info on how to make use of the "do not sell" choice or how the company does not sell consumer information to third parties, a more granular version of "more info: data practices"	An explanation explaining what they will not sell.
do not sell: payment required	The user expect that they would need to pay to prevent the company from selling their data	I think it may take me to another page where they want me to pay for this feature.
do not sell: provide info	The user will be asked to provide more information about themselves in order to make a "do-not-sell" request	I think it would lead me to another page that I would have to fill out to stop the selling of my information.
do not sell: doubted	Participant indicates that they are skeptical that the do not sell request would be honored	It would surprise me if it actually worked to suppress the sale of one's personal information.
garbage	Nonsensical text	good
less privacy	The participant indicates that clicking	Your personal information will be

protection	the icon/link would lead to less privacy protection or another negative outcome but doesn't specify that it's because their data would now be sold	available and spread on the internet.
more info: data practices	More info on how the site collects, uses, and shares user data, a more granular description of privacy policy	The page would take me to a debriefing page of text informing me how the online store will use my personal information.
more info: generic	The generic feeling that they would see more information, without specifying that the information is related to do-not-sell	I think it would redirect me to a different shopping link or supply additional information.
more info: privacy choices	The link will lead to more information talking about how one can protect their own privacy or make use of this site's privacy settings	I think it would lead to a page with the company's privacy agreement. It would tell you steps to take to keep your information private.
more info: products/services	More info on the products and services sold on this website, also includes promotions and discounts	I think it would lead me to a page with more information about how to purchase these shoes.
more privacy protection	The user will enjoy a higher level of privacy protection that does not relate to do not sell, such as less tracking and use of cookies, removing existing collected data, or providing an incognito version of the site	They will not track your behaviors and save it.
new page	The link leads users to a new page or opens up a modal but the response does not specify what may be on this page/modal	It would send me to another webpage.
not sure	The user is not sure what to expect	I am not sure what would happen.
nothing	The user expects nothing would happen if they clicked on the icon/link	Nothing at all. I think they would just waste my time.
opt-out choices	Mention "opt out" in a generic way but does not specify "opt out of selling my personal info," or opt out of other things such as data collection	It would give me an option to opt out.
other	Miscellaneous responses	
privacy	The user will be led to a page with	I think it would take me to a page that

choices: generic	choices/controls that can help protect their privacy, without specifying the privacy control is related to do-not-sell	had an option to keep my privacy or an explanation about what the website does with personal information.
privacy policy	Mention the word "policy" "privacy policy" "transparency statement" "legal statement" or having to agree to such legal terms	Maybe it sends you to a privacy policy page.
scam	The link will lead to a scam, virus, or other malicious content	It could be a phishing link that makes it seem to be safe but it's really not.
spamming	The link leads to settings that would bring the user annoying messages such as unwanted emails	Your IP address and information would go to other sources and then you would receive a bunch of emails from other sources.

Open-ended responses for intentions to click (i.e., responses to “You indicated you would...click on the link, if you noticed it for the first time on this or any other website. Please describe why you selected this answer option.”)

Code	Definition	Example
garbage	nonsensical text	N/A
other	used for responses that do not match existing codes	
against data being sold	The user opposes to the idea that companies can make profits by selling user data	I would not want my personal information to be sold.
commitment to privacy	The icon/link demonstrates the company's commitment to user privacy	It goes to show that the website values their customers' privacy.
curiosity: collected data	The user is curious to find out what data about them is collected by the website	I would like to see what personal information they collect and find out more about it.
curiosity: do-not-sell choices	The user is curious to know more about what options are available for "do not sell my personal info"	To see what options were available to block the selling of my info.
curiosity: do-not-sell practices	The user is curious to know more about what data the website sells or does not sell, how committed the website is about not selling user data	I would be curious to know more about this. I would want to know this information as it pertains to this website and also what it might tell me

	etc.	about any other website without this link.
curiosity: generic	The user expresses a generic curiosity of "checking out what's behind"	I would be curious about what the link would say. It would be easy enough to click on the link and find out.
curiosity: payment	The user is curious to know whether they will be charged to use the do-not-sell control	I am curious about why there is a price tag as an icon. I would want to know if they want us to pay a fee in order for them not to sell our private information.
trust issue	The user is unsure about the website's integrity	I wouldn't trust the site completely as it is my first time using it.
icon stands out	The icon draws the user's attention to it	It is red, which sticks out and is a sign, which also sticks out.
curiosity: important info	The user think what's behind the icon/link is probably something important	I would probably click on the icon; it seems very important to read regarding my personal information.
value my privacy	The user says something along the line of "I value my privacy" "I care about my privacy"	I would want to click on this link because I definitely care about my privacy online.
bad opt-out experience	The user expects that exercising the do-not-sell control would be lengthy and inconvenient	It also seems like it would be a hassle to opt into this service.
limited website usage	The user expects that they won't use the website a lot, and hence very little data about them will be collected	I would not think about it too much, especially if I did not plan on using the website more than one purchase.
more research needed	The user says they need to do more research to know whether the icon/link is worth clicking	I'm not sure exactly what that link means. I would probably want to do a little research or know a little more about what that means before I agreed to it.
no concern: data being sold	The user is not concerned about the practice that websites sometimes sell user data to third-parties	it does not concern me enough or is a big enough threat that I would consider it.
no concern: generic	The user says something along the line of "it doesn't concern me" but does not specify what "it" means	Not usually a concern of mine.
no concern:	The user says they don't really care	I just don't care about my personal

personal info	about their personal information/information collected by a shopping website	information like that, especially not on a shoe vendor's site.
no meaningful control	The user expects that the icon/link will lead to lengthy information with no meaningful control about do-not-sell	The title also made it seem like the link is just a privacy information since it is located under the information section.
phishing concern	The user fears that it might be a phishing link	I am not sure whether it's a phishing link or not.
trust in the website	The user trusts that the website will handle their data well	I have no reason to distrust the website or think they would mishandle my information in any way.
negative consequences	The user worry that they will suffer negative consequences as a result of using this do-not-sell control	I would be worried about potential negative consequences of clicking on this link. For example, the store might give me a harder time when I am requesting a refund or disputing a transaction because they don't like the fact that I disallowed them from selling my personal data.
personal habit	The user has his/her own preferred way of doing something	I don't normally do this for other websites so I might not think so.
location	The location of the icon is easily missed by the user	Especially where right to left reading is concerned it is listed almost last at the lower right in a block of other fairly nondescript information.
usability	The usability of the website will cause the user not want to click	I think it is too much work to click the link.
depends on behaviors	Whether the user decides to click on the icons depends on whether they will purchase something from the site	I haven't entered any personal information so I don't think I would feel a need to click on it. If I had entered any personal information, I might feel differently.
distraction	The user considers clicking on the icons as a distraction from what they are doing	I would probably be too focused on buying the item rather than the "do not sell my information" link.

Open-ended responses for ratings (i.e., responses to “How well does the following icon convey that there is an option to tell a website “do not sell my personal information?” Please explain why you gave this rating.”)

Code	Definition	Example
ambiguous	The user could not get it from the icon that it represents "do not sell my personal information" / The user struggled to interpret the meaning of the icon	This is slightly better, but overall I think I would be confused if I saw this icon.
complicated	The user explicitly mentioned that the icon is complicated	It isn't clear and a bit complicated.
confusing	The user could interpret something out from the icon, but the icon meant things other than "do not sell my personal information"	It's a little misleading but that icon is the most effective so far in terms of implying something about my payment information would not be shared.
convey inaccurate information	The icon conveys message that is not correct or inaccurate, not related to "do not sell personal information" or "personal information"	Reminds me of currency exchange.
icon does not stand out	The icon does not stand out and fails to attract the user's attention	This icon doesn't show as much attention or warning.
icon not sufficient	The icon does not make sense unless accompanied by the link text "do not sell my personal information"	Only if the icon is next to the text "do not sell my personal information'.
icon too small	The icon is too small when zoomed out	It was very small and, again, the icon with the price tag strikes me as ambiguous or misleading.
not conveyed: personal info	The meaning of the icon is somewhat clear, but it is hard to be connected with personal information	It is obvious that the symbol means "stop" and the dollar sign represents money, it is just hard to connect it to one's personal information.
loose connection with privacy	The icon does not convey the concept of data privacy / security	All I see is a money sign, no correlation with privacy.
not conveyed: do not	The icon does not convey the sense of "do not" or "stop"	The dollar sign says money is involved, but no line through it to indicate “No.”

prior knowledge needed	The meaning of the icon needs to be learned over time / through educational campaigns	Another cryptic symbol that would have to be learned.
unclear	too little information is provided, so it is not clear what the participant means	It just doesn't fit.
conveyed: do not	The icon conveys the sense of "stop" "do not" "something is not allowed" "something is prohibited"	This seems closer to something that would make me think it's stopping something or forbidding something.
conveyed: personal info	The icon specifically conveys some idea related to "personal information"	The icon conveys something about selling and the user. People could most likely conclude it's about personal information.
icon is big	The icon is big enough to be seen even when zoomed out	The icon is big bold and in your face.
icon is simple	The icon is simple and not overly complicated	Because it's very straightforward
icon stands out	The icon stands out and can easily grab the user's attention due to some reason, e.g., red color	The red icon with the dollar sign crossed out sends out a visual message and stands out.
meaningful icon	The icon conveys the meaning of "do not sell my personal information" to some extent	If it was a common place I could see people understanding this icon pretty quickly.
dollar sign: negative	The user does not like the dollar sign	Still not perfect. I do not like the dollar sign.
price tag: negative	The user does not like the price tag	The price tag symbol adds no useful visual information to the icon.
stop sign: negative	The user does not like the stop sign	It is hard to tell that the circle is a stop sign so the meaning is confusing
person: negative	The user does not like the little person icon	Somewhat unclear since a symbol of a person doesn't necessarily mean info.
strike through: negative	The user does not like the strike through	The slash symbol means do not go there
red: negative	The user does not like the use of red color	The color red is a cautionary sign and the icon does not look valid or coherent.
money related	The icon conveys some concepts	The icon communicates nothing at all

	related to money or cash	without the accompanying text, other than it's something related to money which could be a million things
pay for do-not-sell	The icon means that consumers need to pay to prevent their information from being sold	When I first saw it I thought it was an option for me to pay to have the website not sell my information. The sentence already has the word "sell" in it, we don't need the dollar sign/tag/stop sign icon.
payment related	The icon is related with payment options or no payment	Ambiguous and misleading. It looks like they want me to pay for something.
sales related	The icon conveys the concept of sale, price, price tag, something is being sold, discounts, coupons, deals	It shows a strike out over the money sign which is ok, but I'd still think it might convey a sale.
shipping related	The icon conveys the concept of shipping	It makes me think it will stop something money related, associated with a price tag or perhaps shipping.
shopping related	The icon conveys concepts related to shopping (stop shopping), buying (stop buying), purchases, cancel order	This icon doesn't really explain the information to not sell my information because it has a price tag in the stop sign. This indicates possibly to stop shopping.
ads related	The icon conveys concepts related to ads	The dollar sign could refer to targeted ads.
selling personal info	The icon conveys the concept of "selling personal info" which is the opposite of do-not-sell	It looks like a generic message, which could mean that they are selling your information, or that it's completely unrelated like for payment information.
dollar sign: positive	The user calls out the dollar sign as a positive element that helps with their interpretation	It's red, which happens to be a very eye catching color plus, it has a dollar sign within it. The lettering is also bolded next to it so it's really hard to miss.
red color: positive	The user calls out the red color as a positive element that attracts their attention	It's red, which happens to be a very eye catching color plus, it has a dollar sign within it. The lettering is also bolded next to it so it's really hard to miss.

stop sign: positive	The user calls out the stop sign as a positive element that helps with their interpretation	Again the red stop sign gave it away.
price tag: positive	The user calls out the price tag as a positive element that helps with their interpretation	Because the icon looks like a red stop sign with a price tag, which could indicate not to sell something but some people might not realize it means not to sell their information.
person: positive	The user calls out the little person icon as a positive element that helps with their interpretation	The icon fully explained it. pepo sign embedded in a stop sign. it is a perfect match.
strike through: positive	The user calls out the strike through as a positive element that helps with their interpretation	Because the way it is crossed out for them not to make money off of my information.

An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites

Hana Habib, Yixin Zou[†], Aditi Jannu, Neha Sridhar, Chelse Swoopes,
Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub[†]
Carnegie Mellon University & [†]University of Michigan
{htq, ajannu, nksridha, cswoopes, acquisti, lorrie, ns1}@andrew.cmu.edu
{yixinz, fschaub}@umich.edu

Abstract

Many websites offer visitors privacy controls and opt-out choices, either to comply with legal requirements or to address consumer privacy concerns. The way these control mechanisms are implemented can significantly affect individuals' choices and their privacy outcomes. We present an extensive content analysis of a stratified sample of 150 English-language websites, assessing the usability and interaction paths of their data deletion options and opt-outs for email communications and targeted advertising. This heuristic evaluation identified substantial issues that likely make exercising these privacy choices on many websites difficult and confusing for US-based consumers. Even though the majority of analyzed websites offered privacy choices, they were located inconsistently across websites. Furthermore, some privacy choices were rendered unusable by missing or unhelpful information, or by links that did not lead to the stated choice. Based on our findings, we provide insights for addressing usability issues in the end-to-end interaction required to effectively exercise privacy choices and controls.

1 Introduction

The dominant approach for dealing with privacy concerns online, especially in the United States, has largely centered around the concepts of notice and consent [56]. Along with transparency, consumer advocates and regulators have asserted the need for consumers to have control over their personal data [22, 28, 41]. This has led some websites to offer privacy choices, such as opt-outs for email communications

or targeted ads, and mechanisms for consumers to request removal of their personal data from companies' databases.

Despite the availability of privacy choices, including mechanisms created by industry self-regulatory groups (e.g., the Digital Advertising Alliance [21]) as well as those mandated by legislation, consent mechanisms appear to have failed to provide meaningful privacy protection [15, 57]. For example, many consumers are unaware that privacy choice mechanisms exist [33, 48, 60]. Additionally, past research has identified usability and noncompliance issues with particular types of opt-outs, such as those for email communications and targeted advertising [24, 35, 40, 42, 55]. Our study builds on prior work by contributing a large-scale and systematic review of website privacy choices, providing deeper insight into how websites offer such privacy choices and why current mechanisms might be difficult for consumers to use.

We conducted an in-depth content analysis of opt-outs for email communications and targeted advertising, as well as data deletion choices, available to US consumers. Through a manual review of 150 English-language websites sampled across different levels of popularity, we analyzed the current practices websites use to offer privacy choices, as well as issues that may render some choices unusable. Our empirical content analysis focused on two research questions:

1. What choices related to email communications, targeted advertising, and data deletion do websites offer?
2. How are websites presenting those privacy choices to their visitors?

We found that most websites in our sample offered choices related to email marketing, targeted advertising, and data deletion where applicable: nearly 90% of websites that mentioned using email communications or targeted advertising in their privacy policy provided an opt-out for that practice, and nearly 75% offered a data deletion mechanism. These choices were provided primarily through website privacy policies, but were often also presented in other locations. Furthermore, our heuristic evaluation revealed several reasons why people may find these choices difficult to use and understand. In over 80% of privacy policies analyzed, the policy text omit-

ted important details about a privacy choice, such as whether a targeted advertising opt-out would stop all tracking on a website, or the time frame in which a request for account deletion would be completed. Though a less frequent occurrence, some policies contained opt-out links that direct the user to a page without an opt-out, or referred to non-existent privacy choices. We further observed a lack of uniformity in the section headings used in privacy policies to describe these choices. Compounded, these issues might make privacy choices hard to find and comprehend.

New regulations, such as the European Union’s General Data Protection Regulation (GDPR) and California’s Consumer Privacy Act (CCPA), aim to address issues with privacy choice mechanisms and include strict requirements for obtaining and maintaining consent for practices like direct marketing, targeted advertising, and disclosure or sale of personal data [25, 50]. Our study contributes a better understanding of the mechanisms websites currently use to provide choices related to these practices, and where they may fall short in helping people take advantage of available choices. Additionally, our analysis provides a foundation for future research into the development of best practices for provisioning privacy choices. These recommendations could build upon changes to the consent experience in the mobile app domain, where research showing the benefits of a uniform interface contributed to changes in permission settings implemented by the Android and iOS platforms [4]. Building new approaches for privacy choice provisioning upon practices that are already prevalent may increase the likelihood of adoption.

2 Privacy Choice Regulatory Framework

As background, we provide an overview of current legislation and industry self-regulatory guidelines related to the types of privacy choices evaluated in this study: opt-outs for email and targeted advertising and options for data deletion.

2.1 Opt-outs for Email Communications

In the United States, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 established national standards for companies that send electronic commercial messages to consumers [29]. It requires companies to provide consumers with a means to opt out of receiving communications, accompanied by a clear and noticeable explanation about how to use the opt-out. Once the commercial message is sent, opt-outs must be available to recipients for at least 30 days, and any opt-out request must be honored within 10 business days. The European Union’s General Data Protection Regulation (GDPR) also grants consumers “the right to object” when their personal data is processed for direct marketing purposes (Art. 21) [25]. Furthermore, the California Consumer Privacy Act (CCPA), which will go into effect in 2020, grants California residents

the right to opt out of having their personal data sold to third parties, such as for marketing purposes [50].

2.2 Opt-outs for Targeted Advertising

Since the early 2000s, industry organizations in the United States and Europe — including the Network Advertising Initiative (NAI), Digital Advertising Alliance (DAA), and Interactive Advertising Bureau Europe (IAB Europe) — have adopted principles and self-regulatory requirements related to practices used in online behavioral advertising [21, 38, 52]. DAA member advertisers are required to provide consumers with the choice to opt out of tracking-based targeted advertising [21]. This requirement applies to data used by the company or transferred to other non-affiliated entities to deliver tailored ads, but not for other collection purposes [46].

The GDPR emphasizes consumers’ consent to the processing of their personal data for purposes that go beyond what is required to fulfill a contractual obligation or immediate business interests. In asking for consent, websites should present a clear, affirmative action, and ask visitors for agreement rather than incorporating the consent into default settings, such as pre-checked boxes (Art. 4). Consent should be in an easily accessible form, using simple, clear language and visualization, if needed; if the consumer is a child, the language must be understandable by a child (Art. 12). Moreover, visitors are allowed to withdraw their consent at any time (Art. 7). Nevertheless, the GDPR does not explicitly state that consent is required for targeted advertising, and ambiguity in Art. 6 may provide leeway for companies to claim a “legitimate business interest” and collect data for targeted advertising without obtaining explicit consent [25].

2.3 Data Deletion Choices

The GDPR also grants consumers whose data is collected in the European Union the “right to be forgotten.” This stipulates that under certain circumstances, companies must comply with consumer requests to erase personal data (Art. 17) [25]. Implementations of the “right to be forgotten” vary from account deletion request forms to the ability of consumers to delete certain information related to their profile.

While no general “right to be forgotten” exists in the United States, some US federal laws contain data deletion requirements for specific contexts. The Children’s Online Privacy Protection Act of 1998 (COPPA), for example, requires online services that collect personal information of children under 13 years old to delete it upon parental request [30]. The CCPA will also give California residents the right to request their personal data be deleted, except in certain circumstances, such as when the information is needed to complete an unfinished transaction [12].

3 Related Work

Our study builds upon prior work that (1) evaluated privacy control mechanisms; and (2) studied consumer attitudes and behaviors related to data collection and use.

3.1 Prior Evaluations of Privacy Choices

The usability of websites' privacy communications and controls has long been problematic [47, 48]. Recent work has shown that privacy policies still exhibit low readability scores [26, 44]. Additionally, most websites fail to provide specific details regarding the entities with which they share data and the purposes for which data is shared [34]. Some consumer advocates argue that current control mechanisms nudge people away from exercising their right to privacy with practices, such as creating a cumbersome route to privacy-friendly options, highlighting the positive outcome of privacy-invasive options, and incentivizing consumers to share more personal data through the framing of control mechanisms [54].

Prior studies have also revealed compliance issues related to privacy control requirements. For example, in the early 2000s the Federal Trade Commissions (FTC) found that privacy controls were not ubiquitously implemented at that time, with only 61% of surveyed websites giving consumers options regarding the collection of their personal information [27]. There is also evidence of noncompliance with the GDPR, as some major websites still deliver targeted ads to European visitors who did not consent to the use of their personal data [19].

However, it seems that companies are adjusting their privacy notice and control mechanisms in response to new legal requirements. Degeling et al. found that, among the more than 6,000 European websites surveyed in 2018, 85% had privacy policies; many websites had updated their privacy policies or started to display cookie consent notices when the GDPR went into effect, likely in response to the GDPR's transparency requirements [20]. Yet, it is unclear whether the changes websites are implementing actually serve to protect consumers. Facebook, for example, was criticized for their post-GDPR privacy changes, as users are still not able to opt out of Facebook's use of behavioral data to personalize their News Feeds or optimize its service [13].

Our analysis primarily focuses on usability issues and does not intend to analyze legal compliance (although the latter is an important direction for future work). Next we highlight key findings of prior usability evaluations regarding email communication opt-outs, targeted advertising opt-outs and data deletion choices, the three types of privacy choices on which our analysis is focused. Our study is the first to survey all three forms of privacy choices in a comprehensive manner through content analysis. Our findings provide an overview of current practices and potential usability pitfalls, with ample implications for making privacy choice mechanisms more uniform and apparent across websites.

3.1.1 Evaluation of Email Communication Opt-outs

Due to the CAN-SPAM Act, many websites offer consumers control over which email messages they receive. An audit of top North American retailers in 2017 by the Online Trust Alliance found that 92% of websites surveyed offered unsubscribe links within messages. However, the study also revealed that compliance issues still exist as some retailers offered broken unsubscribe links, or continued to send emails after the 10-business-days deadline [55]. A 2018 analysis by the Nielsen Norman group revealed usability issues related to unsubscribe options in marketing emails, such as inconspicuous links without visual cues indicating that they are clickable, long and complicated processes involving many check boxes and feedback-related questions prior to the final unsubscribe button, as well as messaging that might annoy or offend users [53]. Our research complements these studies by examining usability issues occurring in unsubscribe mechanisms offered on websites rather than through emails, such as links in privacy policies and account settings.

3.1.2 Evaluation of Targeted Advertising Opt-outs

Existing opt-out tools for targeted advertising include third-party cookie blockers built into web browsers, browser extensions, and opt-out tools provided by industry self-regulatory groups. The effectiveness of these tools varies. Many opt-out options, for example, prevent tailored ads from being displayed but do not opt users out of web tracking [8]. A 2012 study found certain browser extensions and cookie-based tools to be helpful in limiting targeted text-based ads, but the "Do Not Track" option in browsers was largely ineffective [6, 31].

Prior evaluations of targeted advertising opt-out tools have revealed numerous usability issues that can impose a heavy burden on users. For instance, using opt-out cookies is cumbersome, as these cookies need to be manually installed and updated, and may be inadvertently deleted [46]. Browser extensions partially mitigate these issues but introduce other problems. Leon et al. found in 2012 that descriptions of browser extensions were filled with jargon, and participants were not effectively prompted to change their settings when the tool interfered with websites [42]. Some of these tools have since been updated to address usability concerns. Opt-out tools offered by industry self-regulatory groups also exhibit low comprehension, as studies have found that the NAI's description of opt-out cookies led to the misinterpretation that the opt-out would stop all data collection by online advertisers, and DAA's AdChoices icon failed to communicate to web users that a displayed ad is targeted [48, 60]. Moreover, when the AdChoices icon is presented on a mobile device, it tends to be difficult for people to see [33].

Furthermore, studies have identified issues related to non-compliance with self-regulatory guidelines for targeted advertising. Hernandez et al. found in 2011 that among Alexa's US top 500 websites only about 10% of third-party ads used

the AdChoices icon, and even fewer used the related text [35]. Similar noncompliance issues with the enhanced notice requirement were found by Komanduri et al. in a large-scale examination of DAA and NAI members [40]. In 2015, Cranor et al. reported that privacy policies of companies who use targeted advertising did not meet self-regulatory guidelines related to transparency and linking to personally identifiable information [16]. Our analysis complements this prior work by further highlighting practices used by websites that could make advertising opt-outs difficult to use or comprehend.

3.1.3 Evaluation of Data Deletion Choices

Comparatively, there have been fewer evaluations of data deletion mechanisms, likely due to the recency of corresponding legal requirements. The Global Privacy Enforcement Network (GPEN) reported that only half of the websites and mobile apps they evaluated provided instructions for removing personal data from the company’s database in the privacy policy, and only 22% specified the retention time of inactive accounts [34]. An encouraging effort is the JustDelete.me database,¹ which rated the account deletion process of 511 web services. More than half of the websites analyzed (54%) were rated as having an “easy” process for deleting an account from the website. Yet, these ratings only apply to the specific action required to use deletion mechanisms and do not systematically analyze the full end-to-end interaction, which also includes finding and learning available mechanisms and assessing the result of the action, as we do in our study.

3.2 Programmatic Privacy Choice Extraction

Recent efforts in analyzing opt-out mechanisms have utilized automated extraction tools and machine learning. Such tools have been used to evaluate the privacy policies of US financial institutions [17] and descriptions of third-party data collection in website privacy policies [43]. Machine learning classifiers developed by Liu et al. have successfully been used to annotate privacy policy text for certain practices [45]. More directly related to privacy choice mechanisms, Sathyendra et al. and Wilson et al. developed classifiers to identify opt-out choices and deletion options in the privacy policies of websites and mobile apps [58, 62]. Ultimately, these techniques demonstrate the prospect of building tools to extract privacy choices buried in the long text of privacy policies to present them in a more user-friendly manner. However, our manual in-depth analysis of how these choices are presented by websites can identify issues and inform the design of consent mechanisms that better meet users’ needs.

¹ <https://backgroundchecks.org/justdeleteme/>

3.3 Consumer Attitudes and Behavior

Prior studies have shown that consumers are uncomfortable with certain data handling practices commonly used by websites. For example, in a survey conducted by Business Week and Harris Poll in 2000, 78% of respondents were concerned that companies would use their information to send junk emails [9]. Similarly, in another 1999 survey, 70% of respondents wanted to have the choice to be removed from a website’s mailing list [18]. More recently, Murillo et al. examined users’ expectations of online data deletion mechanisms and found that users’ reasons for deleting data were varied and largely depended on the type of service, posing difficulties for a uniform deletion interface adaptable for all services [51].

Most prior work on consumer attitudes and behavior in this area has focused on targeted advertising practices. Internet users consider targeted advertising a double-edged sword: targeted advertising stimulates purchases and is favored by consumers when it is perceived to be personally relevant; yet, it also raises significant privacy concerns due to the large amount of personal data being collected, shared, and used in a nontransparent way [7, 39]. Prior research has shown rich evidence of consumers’ objection to data collection for targeted advertising purposes. In Turov et al.’s 2009 national survey, over 70% of respondents reported that they did not want marketers to collect their data and deliver ads, discounts, or news based on their interests [59]. Similarly, in McDonald and Cranor’s 2010 survey, 55% of respondents preferred not to see interest-based ads, and many were unaware that opt-out mechanisms existed [48]. These findings are supported by qualitative work, such as Ur et al.’s 2012 interview study in which participants generally objected to being tracked [60].

Despite significant privacy concerns, consumers struggle to protect their online privacy against targeted advertising for multiple reasons [14, 42]. Two aspects that limit users’ capabilities in dealing with targeted advertising include the asymmetric power held by entities in the targeted advertising ecosystem, and consumers’ bounded rationality and limited technical knowledge to fully understand and utilize privacy-enhancing technologies [1, 3, 24]. For example, many consumers may not know that ads they see may be based on their email content [48]. Yao et al. showed that mental models about targeted advertising practices contain misconceptions, including conceptualizing trackers as viruses and speculating that trackers access local files and reside locally on one’s computer [63]. These findings highlight the importance of improving the usability of opt-out tools and disclosures of data handling practices, as well as enhancing consumer education.

4 Methodology

We developed an analysis template for the systematic analysis of data deletion, email, and targeted advertising choices offered by websites along multiple metrics. Our analysis in-

cluded websites sampled across different ranges of web traffic that were registered primarily in the United States.

4.1 Template for Analysis

We implemented a comprehensive template in Qualtrics to facilitate standardized recording of data for researchers' manual content analysis of websites. For the purpose of our analysis, we defined opt-outs for email communications as mechanisms that allow users to request that a website stop sending them any type of email message (e.g., marketing, surveys, newsletters). Any mention of an advertising industry website or opt-out tool, as well as descriptions of advertising-related settings implemented by the website, browser, or operating system (e.g., "Limit Ad Tracking" in iOS) was considered as an opt-out for targeted advertising. We identified data deletion mechanisms as a means through which users can delete their account or information related to their account, including via an email to the company.

In completing the template, a member of the research team visited the home page, privacy policy, and account settings of each website examined, and answered the relevant template questions according to the privacy choices available. For each choice identified, we recorded where the privacy choice is located on the website, the user actions required in the shortest path to exercise the choice, and other information about the choice provided by the website. To complete the template, researchers were asked to:

1. Visit the homepage of the website.
2. Note if there was a notice to consumers regarding the use of cookies on the website.
3. Create a user account for the website using an alias and email address provisioned for this analysis.
4. Review any targeted advertising opt-outs on a page linked from the homepage that describes advertising practices (i.e., an "AdChoices" page).
5. Visit the website's privacy policy.
6. Review any email communications in the privacy policy.
7. Review any targeted advertising opt-outs in the policy.
8. Review any data deletion mechanisms in the policy.
9. Note whether the privacy policy mentions Do Not Track.
10. Note any other privacy choices in the privacy policy and linked pages providing privacy information.
11. Review any email communications opt-outs in the user account settings.
12. Review any targeted advertising opt-outs in the user account settings.
13. Review any data deletion mechanisms in the user account settings.
14. Note any other privacy choices in the account settings.

At every stage, researchers also made note of practices for offering privacy controls that seemed particularly detrimental or beneficial to usability throughout the Interaction Cycle, a

framework for describing the end-to-end interaction between a human and a system [5].

To refine the template, our research team conducted six rounds of pilot testing with 25 unique websites from Amazon Alexa's² ranking of top 50 US websites. For every round of piloting, two researchers independently analyzed a small set of websites. We then reconciled disagreements in our analysis, and collaboratively revised the questions in the template to ensure that there was a mutual understanding of the metrics being collected.

4.2 Website Sample

We examined 150 websites sampled from Alexa's ranking of global top 10,000 websites (as of March 22, 2018). To understand how privacy choices vary across a broad range of websites, we categorized these websites based on their reach (per million users), an indicator of how popular a website is, provided by the Alexa API. We selected two thresholds to divide websites and categorized them as: *top websites* (ranks 1 - 200), *middle websites* (ranks 201 - 5,000), and *bottom websites* (ranks > 5,000). These thresholds were identified by plotting websites' reach against their rank, and observing the first two ranks at which reach leveled off. Our analysis included 50 *top*, 50 *middle*, and 50 *bottom* websites randomly selected from each range. We stratified our sample as such, since consumers may spend significant time on websites in the long tail of popularity. The stratified sample enables us to understand the privacy choices provided on low-traffic websites, and how they differ from choices on popular websites.

The ICANN "WHOIS" record of 93 websites in our sample indicated registration in the United States, while other websites were registered in Europe (26), Asia (11), Africa (4), Central America/the Caribbean (2), or contained no country related information (14). In constructing our sample, we excluded porn websites to prevent researchers' exposure to adult content. To simplify our data collection, we also excluded a handful of websites drawn during our sampling that required a non-email based verification step, or sensitive information like a social security number (SSN) or credit card, to create a user account. Due to the language competencies of the research team, we only included websites written in English, or those with English versions available. All websites included in our study were analyzed between April and October 2018. Data collected from our pilot rounds are not included in our analysis. The types of websites included in our sample ranged from popular news and e-commerce websites to university and gaming websites.

Due to the GDPR, many websites were releasing new versions of their privacy policies during the period of our data analysis. In October 2018 we reviewed all websites in our dataset that had been analyzed prior to May 25, 2018, the GDPR effective date, and conducted our analysis again on

²Amazon Alexa Top Sites: <https://www.alexa.com/topsites>

the 37 websites that had updated their privacy policy. Our reported findings are primarily based on the later versions of these policies, but we also compared the pre- and post-GDPR versions for these websites, and highlight differences.

4.3 Data Collection

The researchers involved in data collection went through a training process during which they completed the template for several websites prior to contributing to the actual dataset. To ensure thorough and consistent analysis, two researchers independently analyzed the same 75 (50%) websites sampled evenly across categories. Cohen’s Kappa ($\kappa = 0.82$) was averaged over the questions in which researchers indicated whether or not privacy choice mechanisms were present on the page being analyzed. All disagreements in the analysis were reviewed and reconciled, and the remaining 75 websites were coded by only one researcher. Analyzing one website took 5 to 58 minutes, with an average of 21 minutes spent per website. This variance in analysis time was related to websites’ practices. For example, websites that did not use email marketing or targeted advertising could be reviewed more quickly. To prevent browser cookies, cookie settings, or browser extensions from affecting website content, researchers collected data in Google Chrome’s private browsing mode, opening a new browser window for each website.

4.4 Limitations

The privacy choices we reviewed may not be representative of all websites. Our sample only included English-language websites, which may not be reflective of websites in other languages. We also only included websites from Alexa’s top 10,000 list. Websites with lower rankings may exhibit a different distribution of choices than that observed in our sample. Moreover, in the process of random sampling, we excluded a small number of websites, primarily for financial institutions, that required sensitive personal information (e.g., SSN or credit card) for account registration. Considering the sensitive nature of this type of personal information, these websites may offer privacy choices through different means or offer other choices. However, our sample still includes many websites that collect credit card information and other sensitive personal information, but do not require it for account creation. Despite these exclusions, we are confident the websites we analyzed provide broad coverage of websites’ most prominent practices for offering opt-outs and deletion mechanisms.

Additionally, since our analysis was conducted using US IP addresses, we may not have observed privacy choices available to residents of other jurisdictions (such as the EU) with other legal privacy requirements. Our analysis thus only reflects privacy choices available to US-based consumers.

Lastly, our study cannot provide definite conclusions about how consumers will comprehend and utilize the privacy choices we analyzed. We chose a content analysis approach in order to be able to gain a systematic overview of current practices in provisioning opt-out choices, which was not provided by prior work at this scale. Nonetheless, based on prior opt-out evaluations and design best practices, we hypothesize that certain design choices (e.g., multiple steps to an opt-out choice) will appear difficult or confusing to users. Our findings also surface many other issues that pose challenges to consistent privacy choice design. The effects of these issues on consumers could be studied in future work.

5 Results

Our manual content analysis of 150 websites revealed that privacy choices are commonly available, but might be difficult to find and to comprehend. We identified several factors that likely negatively impact the usability of privacy choices, such as inconsistent placement, vague descriptions in privacy policies, and technical errors.

5.1 Overview of Privacy Policies

Nearly all of the websites in our sample included a link to a privacy policy from the home page. The only websites that did not include a privacy policy were three bottom websites. Of the 147 policies analyzed, 15% (22) were a corporate policy from a parent company. In line with prior findings, comprehension of the text that describes privacy choices requires advanced reading skills [26]. However, about a third of policies in our analysis adopted tables of contents to present the information in a structured way, or linked to separate pages to highlight particular sections of the policy.

Privacy choices text has poor readability. For websites in our sample that had a privacy policy, we recorded the policy text and marked out the portions that described privacy choices. We then conducted a readability analysis using the text analysis service readable.io.

As reported in Table 1, the Flesch Reading Ease Scores (FRES) for text related to email opt-outs, targeted advertising opt-outs, and data deletion choices received means and medians of about 40 on a 0 to 100 point scale (with higher scores indicating easier-to-read text) [32]. The analyzed text for all three types of privacy choices on the Flesch-Kincaid Grade Level (FGL), a grade-based metric, had means and medians around 13, which implies the text requires the audience to have university-level reading abilities. On Flesch’s 7-level ranking system, over 90% of the analyzed privacy choices were described in text that was “very difficult,” “difficult,” or “fairly difficult” to read.

Privacy policies as a whole had better, but not ideal, readability, compared to privacy choice text: our analyzed privacy

	Flesch Reading Ease		Flesch-Kincaid	
	Mean	SD	Mean	SD
Email Comm.	39.54	13.55	13.89	3.40
Targeted Adv.	39.38	15.41	13.72	4.48
Data Deletion	38.98	17.89	14.28	5.40
Privacy Policies	45.80	10.72	10.20	2.44

Table 1: Readability scores for privacy policy text describing email opt-outs, advertising opt-outs, and deletion choices.

policies had a mean FRES of 45.80 and a mean FGL of 10.20, which align with prior readability evaluations of privacy policies, both across domains [26] and for particular categories (e.g., social networking, e-commerce, and healthcare websites [23, 49]). Nevertheless, literacy research suggests materials approachable by the general public should aim for a junior high reading level (i.e., 7 to 9) [36]. These statistics of our analyzed privacy policies and text related to privacy choices, which were all post-GDPR versions, suggest that most of them still fail to comply with the GDPR’s “clear and plain language” requirement, a key principle of transparency.

Some websites use table of contents and support pages.

We also observed that a significant portion of the policies in our sample were organized using a table of contents. Of the 147 privacy policies, 48 (33%) included a table of contents, which provides a road map for users to navigate a policy’s sections. Additionally, 53 (36%) policies linked to secondary pages related to the company’s privacy practices. For example, Amazon and Dropbox have individual pages to explain how targeted advertising works and how to opt-out.

5.2 Presence of Privacy Choices

In this section, we first focus on whether and where choices were present on the websites analyzed. More details about how these choices are described in policies are presented in Section 5.3. We found that privacy choices are commonly offered across all three website tiers. Beyond privacy policies, websites often provide opt-outs and data deletion choices through other mechanisms, such as account settings or email.

Privacy choices are prevalent. All three types of privacy choices were prevalent in our sample. As seen in Table 2, 89% of websites with email marketing or targeted advertising offered opt-outs for those practices, and 74% of all websites had at least one data deletion mechanism. The location of privacy choices across top, middle, and bottom websites is displayed in Figure 1. Top websites were found to provide more privacy choices than middle and bottom websites.

	Email Comm.	Targeted Adv.	Data Deletion
# of sites applicable	112	95	150
# of sites choice present	100	85	111
% of applicable sites	89%	89%	74%

Table 2: Summary of the availability of each type of privacy choice and websites on which they are applicable.

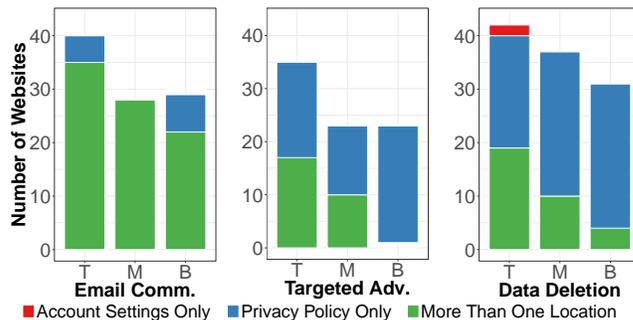


Figure 1: Location of privacy choices for top, middle, and bottom websites. Top websites offered the most privacy choices.

Email opt-outs were links in policies and emails. Most often, opt-outs for email communications were offered in multiple ways. Nearly all (98 of 100) websites offering email communication opt-outs presented the opt-out for emails in the privacy policy; however, only 31 policies included a direct link to the opt-out page, while 70 stated that users could unsubscribe within emails. Additionally, 51 websites had an opt-out in the account settings, the majority of which (33) lead to the same opt-out described in the privacy policy, and 15 websites provided a choice for email communication during account creation.

Advertising opt-outs were links in privacy policies. Websites primarily used their privacy policy to provide opt-outs for targeted advertising. Of 85 websites that offer at least one targeted advertising opt-out, 80 provided them in the privacy policy. Among them, 74 also provided at least one link, while the remaining just described an opt-out mechanism with text, such as “. . . you can opt out by visiting the Network Advertising initiative opt out page.” However, 58 websites had multiple links leading to different opt-out tools, which may cause confusion about which tool visitors should prioritize and what the differences are.

On 26 websites, an “AdChoices” page linked from the homepage described the website’s advertising practices and presented opt-out choices. Among them, 15 used text containing the words “ad choices” to refer to the page; others labeled the page as “interest-based ads,” “cookie information” or “cookie policy.” Additionally, 12 websites included opt-

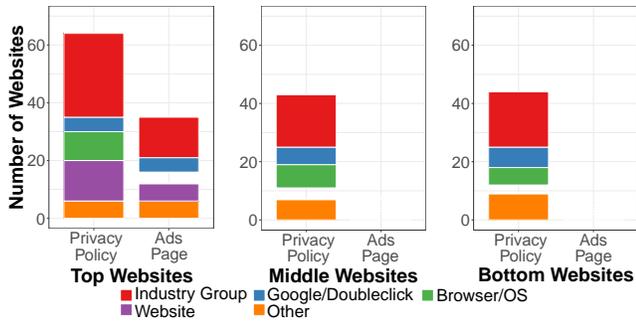


Figure 2: Distribution of different types of targeted advertising opt-outs in privacy policies and “About Ads” pages across top, middle, and bottom websites.

outs in the user account settings, 11 of which led to the same opt-out page presented in the policy.

As seen in Figure 2, many websites referred to opt-out tools provided by advertising industry associations. However, 27% of opt-out links pointing to the DAA or NAI directed visitors to their homepages, instead of their opt-out tools. This creates a substantial barrier for people to opt-out because visitors still need to find the appropriate opt-out tool on the DAA and NAI websites. Conversely, 21 of 22 links to the European Interactive Digital Advertising Alliance (EDAA) in the website policies led directly to the EDAA’s opt-out tool. Less common, some websites provided advertising opt-outs implemented by Google or the website itself. Others provided instructions for adjusting cookie or ad related settings in the browser or operating system, such as the “Limit Ad Tracking” setting in iOS. The use of other services like TrustArc (formerly TRUSTe) or Evidon was also relatively rare.

Data deletion controls were provided in privacy policies and account settings. We observed that 111 websites in our sample (74%) provided data deletion mechanisms to their users, which is higher than the 51% in the sample analyzed by GPEN in 2017 [34]. Among websites offering deletion mechanisms, 75 only provided the choices through the privacy policy, three only displayed them in the user account settings, and 33 provided them through multiple locations. However, even when data deletion choices are described in the privacy policy, only 27 policies included a direct link to a data deletion tool or request form. The more common practice was to offer instructions about how to email a data deletion request, as was done in 81 policies.

The GDPR contributed to more deletion controls. In our sample, 37 websites updated their privacy policy around the GDPR effective date. Four websites added their privacy policies post-GDPR. Most of the 37 websites had already included descriptions of privacy choices before the GDPR effective

date, especially for marketing opt-outs (29 out of 37). In our sample, the GDPR had the greatest impact on data deletion controls, with 13 websites adding instructions for deleting account data to their post-GDPR privacy policy. However, such dramatic change was not observed for marketing and targeted advertising opt-outs.

Websites include other data collection controls. Though less common, some websites described additional privacy-related opt-outs in their privacy policy and account settings. Opt-outs for web analytic services (e.g., Google Analytics) were offered by 21% (31) of websites. Interestingly, 17 websites offered opt-outs for the sharing of personal information with third parties. For example, CNN’s privacy policy³ stated that “We may share the Information with unaffiliated Partners and third parties. . .” and provided a link to an opt-out from such sharing. Additionally, nine websites described controls offered by the website, browser, or operating system related to the use of location history or location data.

Only 28 of the 150 websites analyzed (19%) displayed a cookie consent notice on their home page, alerting users that cookies are being used on the website and getting consent to place cookies in the user’s browser. Among them, only five offered a means to opt out or change cookie related settings. However, as these websites were accessed from US IP addresses, we may have observed different practices than those offered to EU-based visitors. Prior work has found a substantial increase in cookie consent notices on European websites post-GDPR [20].

Do Not Track has low adoption. Of the 150 websites analyzed, only eight (5%) specified that they would honor Do Not Track (DNT), a mechanism that allows users to express that they wish not to be tracked by websites, while 48 (32%) explicitly stated that the website will not honor it [31]. Another 91 (61%) did not specify whether or not they would respect the DNT header, which is in violation of the California Online Privacy Protection Act (CalOPPA) [10].

5.3 Descriptions of Choices in Privacy Policies

In addition to analyzing whether privacy choices are present in privacy policies, we analyzed *how* those choices are presented or described. We found a lack of consensus in the wordings used to present privacy choices. Additionally, many websites provided little information regarding what actually happened when a targeted advertising opt-out or data deletion choice was exercised, thus potentially confusing or misleading users.

There is no dominant wording for section headings. Table 3 summarizes common bigrams and trigrams in policy section headings related to privacy choices. Across policies,

³<https://www.cnn.com/privacy>

N-Gram	Email Comm.	Targeted Adv.	Data Deletion
how we use	9	5	2
opt out	13	7	2
person* data	8	1	10
person* inform*	7	2	13
third part*	0	14	2
we collect	15	7	5
we use	11	5	2
your choic*	11	9	10
your inform*	7	3	10
your right*	9	2	20

Table 3: Bigrams and trigrams occurring in at least 5% of privacy policy section headings. Counts are the number of policies (out of 147) in which a n-gram occurred in the headings of sections containing a privacy choice. Some policies described the same privacy choice under multiple headings, or used multiple n-grams in a heading.

similar headings were used to present all three types of privacy choices, e.g., referring to collection and use of personal data or information, or describing a visitor’s rights or choices. In contrast, the bigram “opt out” more commonly referred to choices related to email communications or targeted advertising. Similarly, advertising opt-outs were sometimes presented under sections describing third parties, which is not as applicable to the other two types of privacy choices. However, no single n-gram occurred in more than 20 of the policies we analyzed. This lack of consistency across websites could make locating privacy choices across websites difficult for visitors. Furthermore, some policies included multiple headings related to privacy choices, which could also potentially add significant burden to visitors.

Most marketing opt-outs are first-party. Among the 98 websites that provided at least one marketing communication opt-out in their privacy policy, 80 websites offered opt-outs from the website’s own marketing or promotions. Additionally, 20 policies stated it is possible to opt out of marketing or promotions from third-party companies, and 19 policies specified that visitors could opt out of receiving website announcements and updates. Other less common forms of emails sent by websites that could be opted out from included newsletters, notifications about user activity, and surveys. Some websites offered opt-outs for different types of communications, such as SMS communications (10) and phone calls (8).

Targeted advertising opt-outs are ambiguous. We observed that privacy policies typically did not describe whether visitors were opting out of tracking entirely or just the display of targeted ads. Only 39 of the 80 websites that offered opt-outs for targeted advertising within their privacy policy

made this distinction within the policy text. Among them, 32 websites explicitly stated that the opt-out only applied to the *display* of targeted ads. This lack of distinction could be confusing to visitors who desire to opt-out of *tracking* on the websites for targeted advertising purposes.

The same ambiguity exists with respect to whether an opt-out applies across multiple browsers and devices. Seventy-three websites’ policies did not specify whether the opt-out would be effective across different devices, and 72 did not clarify whether the opt-out applied across all the browsers a visitor uses.

Data deletion mechanisms vary by website. The data deletion mechanisms presented in the privacy policies of 108 websites varied. Visitors had the option to select certain types of information to be removed from their account on 80 websites. Furthermore, 41 websites offered the option to have the account permanently deleted, and 13 allowed visitors to temporarily suspend or deactivate their account.

How soon the data would actually be deleted was often ambiguous. Ninety of 108 websites offering deletion did not describe a time frame in which a user’s account would be permanently deleted and only four policies stated that information related to the account would be deleted “immediately.” Another three claimed the time frame to be 30 days, and two websites said the deletion process could take up to one year.

5.4 Usability of Privacy Choices

Our analysis included how many steps visitors had to take to exercise a privacy choice. We found that email communications opt-outs, on average, required the most effort. We also recorded specific usability issues on 71 websites (30 top, 23 middle, and 18 bottom) that could make privacy choices difficult or impossible to use, such as missing information and broken links.

Privacy choices require several user actions. We counted user actions as the number of clicks, hovers, form fields, radio buttons, or check boxes encountered from a website’s home page up until the point of applying the privacy choice. Table 4 displays summary statistics related to the shortest path available to exercise choices of each type. Opt-outs for email communications and data deletion choices, on average, contained more user actions, particularly check boxes and form elements, compared to opt-outs for targeted advertising. This is likely due to the reliance on the DAA and NAI opt-out tools, which typically required two or three clicks to launch the tool. Data deletion and email communications choices, on the other hand, often required form fields or additional confirmations. At the extreme end, 38 user actions were required to complete the New York Times’ data deletion request form, which included navigating to the privacy policy, following the link to the request form, selecting a request type, selecting up

	Clicks	Boxes	Hovers	Form	Other	Total
Email Comm.	2.90	1.68	0.38	0.33	0.17	5.32
Targeted Adv.	2.80	0.10	0.25	0.00	0.01	3.16
Data Deletion	2.93	1.05	0.23	1.07	0.05	5.32

Table 4: Average number of actions required in the shortest path to exercise privacy choices, counted from the home page up until, but not including, the action recording the choice (i.e., “save/apply” button).

to 22 check boxes corresponding to different New York Times services, filling in eight form fields, selecting four additional confirmation boxes, and completing a reCAPTCHA.⁴

Policies contain missing, misleading, or unhelpful information. Many choice mechanisms were confusing or impossible to use because of statements in the website’s privacy policy. In six instances, text in the policy referred to an opt-out, but that opt-out did not exist or the website did not provide vital information, such as an email address to which visitors can send privacy requests. Six websites included misleading information in the policy text, such as presenting the Google Analytics opt-out browser extension as an opt-out for targeted advertising,⁵ and omitting mentions of targeted advertising in the privacy policy while providing opt-outs elsewhere on the website. Additionally, seven websites mentioned user accounts in the privacy policy but no mechanisms to create a user account were observed on the website. Two of these cases were TrustedReviews and Space.com, whose policies covered multiple domains, including some with user accounts. These issues appeared in fairly equal frequency across top, middle, and bottom websites.

Some websites had broken choice mechanisms and links. We also recorded 15 instances in which provided links to relevant privacy choice information or mechanisms were broken or directed to an inappropriate location, such as the website’s homepage, or the account settings for a parent website. We further observed that four websites offered choice mechanisms that did not appear to properly function. For example, on Rolling Stone’s email preferences page, selections made by visitors seemed to be cleared on every visit. GamePress’s data deletion request form was implemented by Termly and did not seem to refer to GamePress, making it unclear where and how the form would be processed.

Some websites made poor design choices. We noted several website design choices that may impact the usability of

privacy choices. On ten websites, we observed a privacy policy displayed in an unconventional format, such as in a PDF or in a modal pop-up dialogue, instead of a normal HTML page. This may impact how well visitors can search for privacy choices in a policy. Another design choice that impacted searchability was collapsing the policy text under section headings; keyword search is not effective unless all sections are opened. Five policies also had stylistic issues with their policies, such as including opt-out links that were not clickable or advertisements in the middle of the policy. Some websites offered burdensome pages for managing email communication settings, requiring visitors to individually deselect each type of communication sent by the website. Others placed the option for opting out of all communications *after* a long list of different types of content, rather than before it, making it less visible. For example, Amazon offered this option after listing 79 different communications, which rendered it invisible until scrolling much further down the page.

5.4.1 Aids for privacy choice expression

Conversely, a few websites made additional efforts to make their privacy choices more accessible to visitors. Many opt-outs (such as the Google Ad Settings page) went into effect once a visitor expressed a privacy choice, and did not require the additional step of pressing a confirmation (i.e., “save/apply”). Some, like Metacrawler, centralized the privacy choices related to email communications, targeted advertising, and data deletion into a single section of the policy. Others, including Fronter, were diligent about providing links to related privacy information, such as regulation or the privacy policies of third parties used by the website. To further aid visitors, three websites (BBC, Garena, and LDOCE Online) presented important privacy information in a “Frequently Asked Questions” format. Moreover, Google and Booking.com, provided users with a short video introducing their privacy practices.

6 Improving Privacy Choices

Our findings indicate that certain design decisions may make exercising privacy choices difficult or confusing, and potentially render these choices ineffective. We provide several *design* and *policy* recommendations for improving the usability of web privacy choices. Our recommendations not only serve as concrete guidelines for website designers and engineers, but also have the potential to help policy makers understand current opt-out practices, their deficiencies, and areas for improvement. These suggestions could then be integrated into future guidelines, laws, and regulations.

Our discussion is based on the Interaction Cycle, which divides human interaction with systems into four discrete stages [5]. It serves as a framework to highlight the cognitive and physical processes required to use choice mechanisms,

⁴reCAPTCHA: <https://www.google.com/recaptcha/intro/v3.html>

⁵Google merged its advertising and analytics platforms in July 2018, but the Google Analytics opt-out extension only pertains to analytics tracking.

and in turn synthesizes our findings to address specific usability barriers. We mapped the expression of online privacy choices to the Interaction Cycle as: 1) finding, 2) learning, 3) using, and 4) understanding a privacy choice mechanism.

6.1 Finding Privacy Choices

Use standardized terminology in privacy policies. As noted in Section 5.3, no single n-gram was present in an overwhelming majority of privacy policy section headings in which choices were described, and there was much variation in how websites offered privacy choices. For example, data deletion mechanisms were placed under headings like “What do you do if you want to correct or delete your personal information?” in some policies, but under more general headings like “Your Rights” in others. Even more confusing, some policies contained multiple titles similar to both of these.

Inconsistencies across different privacy policies may make finding specific privacy choices difficult. We recommend that future privacy regulations include requirements for standardized privacy policy section headings. Such guidance exists for privacy notices of financial institutions in the United States, as well as data breach notifications to California residents [11, 61]. Our results highlight the most common terms that websites already use in providing privacy choices, which could serve as a foundation for formulating such guidance.

Unify choices in a centralized location. Websites sometimes offer different opt-out choices on different pages of the website for the same opt-out type. This problem is most salient for targeted advertising opt-outs, which could appear either in privacy policies, account settings, or an individual “AdChoices” page linked to from the home page. Furthermore, some privacy policies did not link to the “AdChoices” page or the account settings where the advertising opt-outs were located. Therefore, by looking at just the privacy policy, which may be where many users would expect to find privacy choices, visitors would miss these opt-outs available to them.

One potential solution is having all types of privacy choices in a centralized location. This can be achieved as a dedicated section in the privacy policy, or even as an individual page with a conspicuous link provided on the home page. However, it will likely require regulatory action for many companies to prioritize reorganizing their current opt-outs in this way.

6.2 Learning How To Use Privacy Choices

Simplify or remove decisions from the process. Another practice that adds to the complexity of exercising opt-outs is the presence of links to multiple tools. For instance, more than one third (58) of our analyzed websites provided links to multiple advertising opt-outs. To simplify the privacy choice process, websites should unify multiple choice mechanisms into a single interface, or provide one single mechanism for a

particular type of privacy choice. If not technically feasible, websites should help visitors distinguish the choices offered by each mechanism.

Ensure all choices in the policy are relevant. The use of one policy for a family of websites might be the reason for some of the points of confusion highlighted in Section 5.4. These corporate “umbrella policies” might explain cases where we observed links from the privacy policy directing to unrelated pages on a parent company’s website, or references to account settings even when the website does not offer mechanisms to create user accounts. While maintaining one policy may be easier for parent companies, this places a substantial burden on visitors to identify the practices that apply to a particular website.

To mitigate such issues, companies should carefully check if the information provided in the privacy policy matches the websites’ actual practices. If an umbrella policy is used across multiple websites, practices should be clearly labelled with the websites to which they are applicable. Regulatory authorities should further exert pressure by emphasizing the necessity of having accurate privacy policies and conducting investigations into compliance.

6.3 Using Privacy Choices

Simplify multi-step processes. We noted that privacy choices typically require multiple steps, which may frustrate and confuse users. As described in Section 5.4, our analyzed privacy choices required an average of three to five user actions prior to pressing a button to apply the choice, assuming the visitor knew which pages to navigate to in advance. On the extreme end, completing one deletion request form required 38 user actions, as the interface included several boxes related to different services offered by the website. Though this type of interface allows users to have greater control, websites should also have a prominent “one-click” opt-out box available to visitors.

It is also conceivable that many companies may deliberately make using privacy choices difficult for their visitors. In this case, it is up to regulators to combat such “dark patterns.” [2, 54] Though it may be unrealistic to set a threshold for the maximum number of user actions required to exercise a privacy choice, regulators should identify websites where these processes are clearly purposefully burdensome and take action against these companies. This would both serve as a deterrent to other companies and provide negative examples. Precedents of such regulatory action have emerged, such as a ruling by the French Data Protection Authority (the “CNIL”) which found that Google fails to comply with the GDPR’s transparency requirement as its mobile phone users need “up to five or six actions to obtain the relevant information about the data processing” when creating a Google account [37].

Some of our analyzed websites have already provided exemplary practices to simplify privacy choices, e.g., automatically applying privacy choices once the user selects or deselects an option, rather than requiring the user to click an additional “save” or “apply” button. Clicking an additional button may not be intuitive to users, especially if it is not visible without scrolling down the page. Removing this extra step would avoid post-completion errors, in which a user thinks they have completed privacy choice, but their choice is not registered by the website. A requirement that all changes in privacy settings must be automatically saved could be integrated into regulations and related guidelines. However, any changes should be made clear to the user to avoid accidental changes.

Provide actionable links. Our findings show that the use of links pointing to privacy choices was not ubiquitous, and varied substantially across different types of privacy choices; 93% of websites that offered the choice to opt out of targeted advertising provided at least one link, whereas the percentage for email communication opt-out and data deletion choice was 32% and 24% respectively. Websites that do not provide links usually provide text explanations for the opt-out mechanisms instead. However, visitors may not follow the text instructions if significant effort is required, such as checking promotional emails in their personal inbox for the “unsubscribe” link, or sending an email to request their account to be deleted. We also found that some websites may not provide sufficient guidance to support exercising a privacy choice.

Our findings point to the necessity to enhance the actionability of privacy choices by providing links. However, there should be a careful decision about how many links to include and where to place them. Ideally, only one link for one particular type of opt-out should be provided. When multiple links are presented on the same page, there needs to be sufficient contextual information to help users distinguish these links. Of equal importance is the functionality of provided links. In our analysis, we observed a few instances in which the provided links were broken, directed to an inappropriate location, or had styling that easily blended in with text. These practices reduce the actionability of the corresponding privacy choice and negatively impact the user experience.

6.4 Understanding Privacy Choices

Describe what choices do. We found that privacy policies did not provide many details that informed visitors about what a privacy choice did, particularly in the cases of targeted advertising opt-outs and data deletion choices. Among all websites that provided targeted advertising opt-outs, fewer than 15% distinguished opting out of tracking from opting out of the display of targeted ads, or indicated whether the opt-out was effective on just that device or browser or across all their devices and browsers. Similarly, among all websites

that provided data deletion choices, only 19% stated a time frame for when the account would be permanently deleted.

Future regulations could stipulate aspects that must be specified when certain opt-outs are provided (e.g., the device that the opt-out applies to). This may reduce instances where visitors form expectations that are misaligned with a companies’ actual practices.

7 Conclusion

We conducted an in-depth empirical analysis of data deletion mechanisms and opt-outs for email communications and targeted advertising available to US consumers on 150 websites sampled across three ranges of web traffic. It is encouraging that opt-outs for email communications and targeted advertising were present on the majority of websites that used these practices, and that almost three-quarters of websites offered data deletion mechanisms. However, our analysis revealed that presence of choices is not the same as enabling visitors to execute the choice. Through our holistic content analysis, we identified several issues that may make it difficult for visitors to find or exercise their choices, including broken links and inconsistent placement of choices within policies. Moreover, some policy text describing choices is potentially misleading or likely does not provide visitors with enough information to act. Design decisions may also impact the ability of visitors to find and exercise available opt-outs and deletion mechanisms. We offer several design and policy suggestions that could improve the ability of consumers to use consent and privacy control mechanisms.

Acknowledgments

This project is funded by the National Science Foundation under grants CNS-1330596 and CNS-1330214. We wish to acknowledge all members of the Usable Privacy Policy Project (www.usableprivacy.org) for their contributions.

References

- [1] Alessandro Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the Conference on Electronic Commerce (EC)*, pages 21–29, 2004.
- [2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users’ choices online. *ACM Computing Surveys (CSUR)*, 50(3):44, 2017.

- [3] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy (S&P)*, 3(1):26–33, 2005.
- [4] Hazim Almuhiemedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 787–796, 2015.
- [5] Terence S Andre, H Rex Hartson, Steven M Belz, and Faith A McCreary. The user action framework: A reliable foundation for usability engineering support tools. *International Journal of Human-Computer Studies*, 54(1):107–136, 2001.
- [6] Rebecca Balebako, Pedro Leon, Richard Shay, Blase Ur, Yang Wang, and Lorrie Faith Cranor. Measuring the effectiveness of privacy tools for limiting behavioral advertising. In *Proceedings of the Web 2.0 Security and Privacy Workshop (W2SP)*, 2012.
- [7] Alexander Bleier and Maik Eisenbeiss. The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3):390–409, 2015.
- [8] Sophie C Boerman, Sanne Kruikemeier, and Frederik J Zuiderveen Borgesius. Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, 46(3):363–376, 2017.
- [9] Bloomberg Businessweek. Business Week/Harris Poll: A Growing Threat. page 96, 2000.
- [10] California Legislative Information. Online privacy protection act of 2003 - California business and professions code sections 22575-22579, 2003.
- [11] California State Government. California civ. code s. 1798.82(a), 2003. https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.82.
- [12] California State Legislature Website. SB-1121 California consumer privacy act of 2018, 2018. https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.
- [13] Josh Constine. A flaw-by-flaw guide to Facebook’s new GDPR privacy changes, May 2018. <https://techcrunch.com/2018/04/17/facebook-gdpr-changes/>.
- [14] Lorrie Faith Cranor. Can users control online behavioral advertising effectively? *IEEE Security & Privacy (S&P)*, 10(2):93–96, 2012.
- [15] Lorrie Faith Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications & High Technology Law*, 10:273, 2012.
- [16] Lorrie Faith Cranor, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au. Are they worth reading? An in-depth analysis of online trackers’ privacy policies. *A Journal of Law and Policy for the Information Society*, 11:325, 2015.
- [17] Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur. A large-scale evaluation of U.S. financial institutions’ standardized privacy notices. *Transactions on the Web*, 10(3):17, 2016.
- [18] Lorrie Faith Cranor, Joseph Reagle, and Mark S Ackerman. Beyond concern: Understanding net users’ attitudes about online privacy. Technical report, TR 99.4.1, AT&T Labs-Research, 1999.
- [19] Paresh Dave. Websites and online advertisers test limits of European privacy law, 2018. <https://www.reuters.com/article/us-europe-privacy-advertising-gdpr/websites-and-online-advertisers-test-limits-of-european-privacy-law-idUSKBN1JS0GM>.
- [20] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We value your privacy... now take some cookies: Measuring the GDPR’s impact on web privacy. In *Proceedings of Network and Distributed System Security Symposium (NDSS ’19)*, 2019.
- [21] Digital Advertising Alliance. Self-regulatory principles for online behavioral advertising, July 2009. <http://digitaladvertisingalliance.org/principles>.
- [22] Electronic Frontier Foundation. Do not track. <https://www.eff.org/issues/do-not-track>.
- [23] Tatiana Ermakova, Benjamin Fabian, and Eleonora Babina. Readability of privacy policies of healthcare websites. In *Proceedings of Wirtschaftsinformatik*, pages 1085–1099, 2015.
- [24] José Estrada-Jiménez, Javier Parra-Arnau, Ana Rodríguez-Hoyos, and Jordi Forné. Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, 100:32–51, 2017.
- [25] European Commission. 2018 reform of EU data protection rules. <https://ec.europa.eu/commission/>

- priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
- [26] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence (WI)*, pages 18–25, 2017.
- [27] Federal Trade Commission. Privacy online: Fair information practices in the electronic marketplace, May 2000. <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.
- [28] Federal Trade Commission. Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers, March 2012. <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.
- [29] Federal Trade Commission. CAN-SPAM Act: A compliance guide for business, March 2017. <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>.
- [30] Federal Trade Commission. Children’s online privacy protection rule: A six-step compliance plan for your business, June 2017. <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>.
- [31] Roy T Fielding and David Singer. Tracking preference expression (DNT). W3C candidate recommendation, 2017. <https://www.w3.org/TR/tracking-dnt/>.
- [32] Rudolf Franz Flesch. *Art of Readable Writing*. Harper, 1949.
- [33] Stacia Garlach and Daniel Suthers. ‘I’m supposed to see that?’ AdChoices usability in the mobile environment. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*, 2018.
- [34] Global Privacy Enforcement Network. GPEN Sweep 2017: User controls over personal information, October 2017. <https://www.privacyenforcement.net/sites/default/files/2017%20GPEN%20Sweep%20-%20International%20Report.pdf>.
- [35] J Hernandez, A Jagadeesh, and J Mayer. Tracking the trackers: The AdChoices icon, 2011. <http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon>.
- [36] Mark Hochhauser. Lost in the fine print: Readability of financial privacy notices, July 2001. <https://www.privacyrights.org/blog/lost-fine-print-readability-financial-privacy-notices-hochhauser>.
- [37] Hunton Andrews Kurth LLP. CNIL fines Google €50 million for alleged GDPR violations, January 2019. <https://www.huntonprivacyblog.com/2019/01/23/cnil-fines-google-e50-million-for-alleged-gdpr-violations/>.
- [38] IAB Europe. EU framework for online behavioural advertising, April 2011. https://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf.
- [39] Hyejin Kim and Jisu Huh. Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising*, 38(1):92–105, 2017.
- [40] Saranga Komanduri, Richard Shay, Greg Norcie, and Blase Ur. AdChoices? Compliance with online behavioral advertising notice and choice requirements. *A Journal of Law and Policy for the Information Society*, 7, 2011.
- [41] Neelie Kroes. Online privacy – reinforcing trust and confidence, June 2011. http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm.
- [42] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Faith Cranor. Why Johnny can’t opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, 2012.
- [43] Timothy Libert. An automated approach to auditing disclosure of third-party data collection in website privacy policies. In *Proceedings of the World Wide Web Conference (The Web Conference)*, pages 207–216, 2018.
- [44] Thomas Linden, Hamza Harkous, and Kassem Fawaz. The privacy policy landscape after the GDPR. *arXiv preprint arXiv:1809.08396*, 2018.
- [45] Frederick Liu, Shomir Wilson, Peter Story, Sebastian Zimmeck, and Norman Sadeh. Towards automatic classification of privacy policy text. Technical report, CMU-ISR-17-118R, Carnegie Mellon University, 2018.

- [46] Jonathan R Mayer and John C Mitchell. Third-party web tracking: Policy and technology. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2012.
- [47] Aleecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *A Journal of Law and Policy for the Information Society*, 4:543, 2008.
- [48] Aleecia M McDonald and Lorrie Faith Cranor. Americans’ attitudes about internet behavioral advertising practices. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*, 2010.
- [49] Gabriele Meiselwitz. Readability assessment of policies and procedures of social networking sites. In *International Conference on Online Communities and Social Computing (OCSC)*, pages 67–75. Springer, 2013.
- [50] Michael Morgan, Daniel Gottlieb, Matthew Cin, Jonathan Ende, Amy Pimentel, and Li Wang. California enacts a groundbreaking new privacy law, June 2018. <https://www.mwe.com/en/thought-leadership/publications/2018/06/california-enacts-groundbreaking-new-privacy-law>.
- [51] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. “If I press delete, it’s gone” - User understanding of online data deletion and expiration. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 329–339, 2018.
- [52] Network Advertising Initiative. NAI code of conduct, 2018. https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.
- [53] Nielsen Norman Group. Top 10 design mistakes in the unsubscribe experience, April 2018. <https://www.nngroup.com/articles/unsubscribe-mistakes/>.
- [54] Norwegian Consumer Council. Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy, June 2018. <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.
- [55] Online Trust Alliance. Email marketing & unsubscribe audit, December 2017. <https://otalliance.org/system/files/files/initiative/documents/2017emailunsubscribeaudit.pdf>.
- [56] Joel R Reidenberg, N Cameron Russell, Alexander J Callen, Sophia Qasir, and Thomas B Norton. Privacy harms and the effectiveness of the notice and choice framework. *I/S: A Journal of Law and Policy for the Information Society (ISJLP)*, 11:485, 2015.
- [57] John A Rothchild. Against notice and choice: The manifest failure of the proceduralist paradigm to protect privacy online (or anywhere else). *Cleveland State Law Review*, 66:559, 2017.
- [58] Kanthashree Mysore Sathyendra, Shomir Wilson, Florian Schaub, Sebastian Zimmeck, and Norman Sadeh. Identifying the provision of choices in privacy policy text. In *Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2017.
- [59] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. Americans reject tailored advertising and three activities that enable it. 2009. <https://ssrn.com/abstract=1478214.143>.
- [60] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2012.
- [61] U.S. Federal Register 74. Final model privacy form under the Gramm-Leach-Bliley act, 2009.
- [62] Shomir Wilson, Florian Schaub, Frederick Liu, Kanthashree Mysore Sathyendra, Daniel Smullen, Sebastian Zimmeck, Rohan Ramanath, Fei Liu, Norman Sadeh, and Noah A Smith. Analyzing privacy policies at scale: From crowdsourcing to automated annotations. *Transactions on the Web*, 13(1):1:1–1:29, 2019.
- [63] Yaxing Yao, Davide Lo Re, and Yang Wang. Folk models of online behavioral advertising. In *Proceedings of the Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*, pages 1957–1969, 2017.

A Websites Analyzed

Top Websites

adobe.com, aliexpress.com, amazon.com, ask.com, bbc.co.uk, bet9ja.com, booking.com, buzzfeed.com, cnn.com, coinmarketcap.com, craigslist.org, dailymail.co.uk, dailymotion.com, diply.com, discordapp.com, dropbox.com, ebay.com, etsy.com, facebook.com, github.com, google.com, indeed.com, mediafire.com, mozilla.org, nih.gov, nytimes.com, paypal.com, pinterest.com, providr.com, quora.com, reddit.com, roblox.com, rumble.com, salesforce.com, scribd.com, slideshare.net, spotify.com, stackexchange.com, stackoverflow.com, thestartmagazine.com, tumblr.com, twitch.tv, twitter.com, w3schools.com, whatsapp.com, wikia.com, wikihow.com, wikipedia.org, wordpress.com, yelp.com

Middle Websites

17track.net, abcnews.go.com, avclub.com, babbel.com, bbb.org, cbc.ca, colorado.edu, desmos.com, file-upload.com, funsafetab.com, furaffinity.net, gamepress.gg, huawei.com, indiewire.com, intel.com, internshala.com, kijiji.ca, ladbible.com, mit.edu, myspace.com, news24.com, openclassrooms.com, opera.com, pathofexile.com, php.net, pixiv.net, poloniex.com, python.org, qwant.com, researchgate.net, rollingstone.com, runescape.com, sfgate.com, signup-genius.com, space.com, speedtest.net, theadvocate.com, trustedreviews.com, tufts.edu, ucl.ac.uk, umd.edu, ups.com, upsc.gov.in, utah.edu, wattpad.com, wikiwand.com, worldbank.org, worldoftanks.com, yifysubtitles.com, zapmeta.ws

Bottom Websites

abebooks.com, adorama.com, artsy.net, bovada.lv, cj.com, classlink.com, coreldraw.com, dotloop.com, elitedaily.com, eurowings.com, fangraphs.com, filmapi.com, findlaw.com, fin-eartamerica.com, foodandwine.com, frontier.com, garena.com, gear4music.com, ghaffa.com, hide.me, hsn.com, hsreplay.net, junkmail.co.za, justjared.com, kodi.tv, ldoceonline.com, letgo.com, lpu.in, majorgeeks.com, metacrawler.com, momjunction.com, mr-johal.com, ni.com, notepad-plus-plus.org, ou.edu, phys.org, playhearthstone.com, priceprice.com, rarlab.com, rice.edu, shein.in, statistic-showto.com, stocktwits.com, theathletic.com, tradingeconomics.com, uottawa.ca, uptostream.com, usgamer.net, volvocars.com, wimp.com

B Website Analysis Template

Step 1: Visit the homepage of the website

1. Please enter the name of the website (use the format "google.com").
2. Did you see a notice for consumers that is an "opt-in" to the website's privacy policy and terms of conditions (including the use of cookies)? [Yes, and it included a way to opt-out or change settings; Yes, but it did not include a way opt-out or change settings; No]
3. Is there an option on the website to create a user account? [Yes, No, Other (please specify)]

Logic: The following two questions are displayed if Q3 = Yes

Step 2: Please create a user account for this site.

4. Do you see the option to opt out of the site's marketing during the account creation process? [Yes, No, Other (please specify)]

5. Does the website have account settings? [Yes, No, Other (please specify)]

Step 3: Look for an "about advertising" or "ad choices" related link on the home page. Click on the "about advertising" or "ad choices" link if it is there.

6. Is there an "about advertising" or "ad choices" related link on the home page? [Yes, and it works; Yes, but it's broken; No]

Logic: The following question is displayed if Q6 = Yes, and it works or Q6 = Yes, but it's broken

7. What was this link labeled? [Ad Choices, Something else (copy label)]

Logic: The following three questions are displayed if Q6 = Yes, and it works

8. Where does the link direct you to? [Somewhere inside privacy policy, Somewhere inside account settings, An individual web page within the site that introduces OBA opt-outs, DAA's webpage, NAI's webpage, TrustE/TrustArc website, Other group's webpage]

9. By which parties are the advertising opt-outs on this page implemented? Include all entities that are linked to on the page. (select all that apply) [DAA, DAA of Canada (DAAC), European Interactive Digital Advertising Alliance (EDAA), Australian Digital Advertising Alliance (ADAA), NAI, TrustE/TrustArc service, The website, The browser or operating system (e.g., instructions to clear cookies or reset device advertising identifier), Google/DoubleClick, Other groups (please specify), There are no advertising opt-outs on this page]

10. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the opt-outs provided on this page?

11. What is the default setting for the opt-outs on this page (e.g., types of emails or ads already opted out of)? If none, enter 'NA'.

Step 4: Now please go back to the homepage if you are not already there.

12. Could you find the link to the site's privacy policy, or a page equivalent to a privacy policy? [Yes, and the link works; Yes, but the link is broken; No]

Logic: The following six questions are displayed if Q12 = Yes, and the link works

Step 5: Visit the website's privacy policy, or the page equivalent to a privacy policy. Some websites may call their privacy policy something else.

13. Please copy and paste the URL for this page. Retrieve this policy through the policy retrieval tool.
14. Please copy and paste the title of the site's privacy policy.
15. Does the privacy policy (or equivalent page) have a table of contents? [Yes, No, Other (please specify)]

Step 6.1: Next, do a search for "marketing," "e-mail," "email," "mailing," "subscribe," "communications," "preference" or "opt" in the privacy policy to look for marketing opt-outs. Also skim through the policy headings to double check.

16. Does the privacy policy say that the site sends marketing or other types of communications (including email)? [Yes, the site sends communications, No, the site does not send communications, Not specified in the privacy policy, Other (please specify)]
17. Does the privacy policy have text about how to opt out of the site's marketing? [Yes, No, Not applicable (the site doesn't send marketing messages), Other (please specify)]

Logic: The following six questions are displayed if Q16 = Yes

18. Please copy and paste the highest level heading in the policy where it describes how to opt out of the site's marketing.
19. Please copy and paste the paragraph(s) in the policy describing how to opt out of the site's marketing in the privacy policy.
20. According to the privacy policy, what types of communications can users opt out of receiving? (Make a note in the comment section if the first and third party emails are not clearly distinguished) [Newsletters, First-party marketing/promotional emails, Third-party marketing/promotional emails, User activity updates, Site announcements, Surveys, Mails, Phone calls, Text Messages/SMS, Other (please specify), None of the above]
21. According to the privacy policy, what types of communications users CANNOT opt out of? [Newsletters, First-party marketing/promotional emails, Third-party marketing/promotional emails, User activity updates, Site announcements, Surveys, Mails, Phone calls, Text Messages/SMS, Other (please specify), None of the above]

22. Does the privacy policy specify whether you can opt-out of marketing within the e-mails? [Yes, you can opt-out within the e-mails; Yes, but you can't opt-out with the e-mails; No, it wasn't specified]

23. Does the privacy policy include any links to marketing opt-outs? [Yes, there's one link to a marketing opt-out; Yes, there're multiple links to a marketing opt-out; No]

Logic: The following four questions are displayed if Q23 = Yes, there's one link to a marketing opt-out or Q23 = Yes, there're multiple links to a marketing opt-out

Step 6.2: Next, one by one click the links to the marketing opt-out links.

24. Do any of the links in the privacy policy to the marketing opt-outs work? [Yes, they all work; Some work, but some do not; No, none of the links to the marketing opt-outs work]

25. Please copy and paste the URL(s) of the working links.

26. Please copy and paste the URL(s) of the broken links.

27. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the marketing opt-outs provided in the privacy policy?

Logic: The following two questions are displayed if Q12 = Yes, and the link works

Step 7.1: Next, do a search for "advertising," "ads," in the privacy policy in order to find whether the site has targeted advertising and their related opt-outs. Also skim through the policy headings to double check

28. According to the privacy policy, does the website have targeted advertising? [Yes, the policy states there is targeted advertising; No, the policy states the website does not have targeted advertising; Not specified by the privacy policy]

29. Does the privacy policy page have text about how to opt out of the site's targeted advertising? [Yes, No, Not applicable (the site doesn't use OBA), Other (please specify)]

Logic: The following seven questions are displayed if Q28 = Yes

30. Please copy and paste the highest level heading in the policy where it describes how to opt out of OBA.

31. Please copy and paste the paragraph(s) in the policy describing how to opt out of OBA.

32. According to the text of the privacy policy page, what can users opt out from related to OBA/tracking? [OBA only, Tracking, Not specified, Other (please specify)]
33. Does the privacy policy page say whether the OBA opt-outs located in the privacy policy will be effective across different browsers? [Yes, the policy says they will be effective across different browsers; Yes, but the policy says there're for current browser only; Not specified by the privacy policy; Other (please specify)]
34. Does the privacy policy page say whether the OBA opt-outs located in the privacy policy will be effective across different devices? [Yes, the policy says they will be effective across different device; Yes, but the policy says there're for current device only; Not specified by the privacy policy; Other (please specify)]
35. By which parties are the OBA opt-outs mentioned by the privacy policy implemented? Include all entities that are linked to from the privacy policy. [DAA, DAA of Canada (DAAC), European Interactive Digital Advertising Alliance (EDAA), Australian Digital Advertising Alliance (ADAA), NAI, TrustE/TrustArc service, The website, The browser or operating system (e.g., instructions to clear cookies or reset device advertising identifier), Google/DoubleClick, Other groups (please specify)]
36. Does the privacy policy page include any links to an OBA opt-out? [Yes, there is one link to an OBA opt-out; Yes, there're multiple links to different OBA opt-outs; Yes, there're multiple links to same OBA opt-out; No]

Logic: The following four questions are displayed if Q35 = Yes, there is one link to an OBA opt-out or Q35 = Yes, there're multiple links to different OBA opt-out

Step 7.2: Next, one by one click the links to the OBA opt-outs in the privacy policy.

37. Do any of the links in the privacy policy to the OBA opt-outs work? Note: Count links with different text and the same URL as multiple links. Include links from the privacy policy and one layer of linked pages as well. [Yes, they all work; Some work, but some do not; No, none of the OBA opt-out links work]
38. Please copy and paste the URL(s) of the working links. Place each URL on its own line.
39. Please copy and paste the URL(s) of the broken links. Place each URL on its own line.
40. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the OBA opt-outs provided in the privacy policy?

41. What is the default setting for the OBA opt-outs in the privacy policy (e.g., types of emails or ads already opted out of)? If none, enter 'NA'.

Logic: The following question is displayed if Q12 = Yes, and the link works

Step 8.1: Next, do a search for “delete,” “deletion,” “closing account,” “remove” or similar terms in the privacy policy in order to find data deletion choices. Also skim through the policy headings to double check.

42. Is there any information in the privacy policy that introduces how to delete your account data? [Yes, No, Other (please specify)]
43. Please copy and paste the highest level heading in the policy where it describes how to delete account data.
44. Please copy and paste the paragraph(s) in the policy where it describes how to delete account data.
45. According to the privacy policy, what actions can users perform related to data deletion? [Delete their account permanently, Suspend/deactivate their account (data will not be permanently deleted right away), Choose specific types of data to be deleted from their account, Not specified, Other (please specify)]
46. Please copy and paste the specific types of data indicated in the privacy policy.
47. According to the privacy policy, does the website suspend or deactivate your account before deleting it? [Yes, the policy says your account will be suspended; No, the policy says your account will be deleted after a certain amount of time; Not specified in the policy; Other (please specify)]
48. According to the privacy policy, after how long will the data be permanently deleted? [Not specified, Immediately, One week, 30 days, 60 days, 90 days, 6 months, Other (please specify)]
49. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion out of all the data deletion options?
50. Does the privacy policy include any links to delete your account data? [Yes, there's one link; Yes, there're multiple links; No]

Logic: The following three questions are displayed if Q50 = Yes, there're one link or Q50 = Yes, there're multiple links

Step 8.2: Next, one by one click the links to the data deletion choices.

51. Does the link in the privacy policy to the data deletion choice work? [Yes, they all work; Some work, but some do not; No, they're all broken]
52. Please copy and paste the URL(s) of the working links.
53. Please copy and paste the URL(s) of the broken links.

Logic: The following five questions are displayed if Q11 = Yes, and the link works

Step 9: Next, search for "Do Not Track" or "DNT" in the privacy policy.

54. Will the website honor DNT requests? [Yes, No, Not specified in the privacy policy]

Step 10: Next, skim through the policy for things users can opt-out of. Adjust your previous answers if necessary and complete the following questions.

55. Did you find any other type of opt-outs in the privacy policy? [Yes, No]
56. What other things can users opt out from at this site as described in the privacy policy? [Device info; All first-party cookies; Location history; Profile activities/inferred interests; Sharing with third parties; Google Analytics; Other (please specify); None of the above]
57. When you are skimming through the privacy policy, could you find any other pages that aim to explain the privacy policy or the privacy and data practices of the company in general? [Yes, and the link works; Yes, but the link is broken; No; Other (please specify)]
58. Please copy and paste the URL of the link(s).
59. Did the privacy policy describe the location of a marketing or communications opt out located in the account settings? [Yes, No]

Step 11: Go to this described location in the account settings or look through the main levels of the account settings for marketing, email, or communication choices. Click links which seem to indicate user choice or preferences.

60. Is there any marketing opt-out located in the account settings? [Yes, No, Not applicable (the site doesn't send email/marketing messages), Other (please specify)]

61. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion to this marketing opt-out?

62. What is the default setting for the marketing opt-outs in the account settings (e.g., types of emails or ads already opted out of)? If none, enter 'NA'.

63. Is it the same marketing opt-out page that was presented in the privacy policy? [Yes; No, it's a different marketing opt-out page; There was no marketing opt-out described in the privacy policy; Other (please specify)]

Logic: The following question is displayed if Q63 is not "Yes"

64. What types of communications can users opt out of from in the account settings? [Newsletters, First-party marketing/promotional emails, Third-party marketing/promotional emails, User activity updates, Site announcements, Surveys, Mails, Phone calls, Text Messages/SMS, Other (please specify), None of the above]

65. Did the privacy policy describe the location of an OBA opt-out located in the account settings? [Yes, No]

Step 12: Go to this described location in the account settings or look through the main levels of the account settings for advertising choices. Click links which seem to indicate user choice or preferences.

66. Is there any OBA opt-out located in the account settings? [Yes, No, Not applicable (the site doesn't use OBA), Other (please specify)]

67. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion to this targeted advertising opt-out?

68. Is it the same opt-out page that was presented in the privacy policy? [Yes; No, it's a different OBA opt-out page; There was no OBA opt-out described in the privacy policy; Other (please specify)]

Logic: The following four questions are displayed if Q68 is not "Yes"

69. By which parties is the OBA opt-out in the account settings implemented? Include all entities that are linked to from the account settings. [DAA, DAA of Canada (DAAC), European Interactive Digital Advertising Alliance (EDAA), Australian Digital Advertising Alliance (ADAA), NAI, TrustE/TrustArc service, The website, The browser or operating system (e.g., instructions to clear cookies or reset device advertising identifier), Google/DoubleClick, Other groups (please specify)]

- 70. What can users opt out from related to OBA/tracking from the account settings? [OBA only (users will still be tracked), Tracking, Not specified, Other (please specify)]
- 71. According to the information provided, will the OBA opt-out in the account settings be effective across different browsers? [Yes; No, it's for current browser only; Not specified; Other (please specify)]
- 72. According to the information provided, will the OBA opt-out in the account settings be effective across different devices? [Yes; No, it's for current device only; Not specified; Other (please specify)]
- 73. Did the privacy policy describe the location of a data deletion choice in the account settings? [Yes, No]

Step 13: Go to this described location in the account settings or look through the main levels of the account settings for data deletion choices. Click links which seem to indicate user choice or preferences.

- 74. Is there any data deletion option located in the account settings? [Yes, No, Other (please specify)]
- 75. How many user actions (e.g., clicks, form fields, hovers) are in the shortest path to completion to this data deletion option?
- 76. Is it the same data deletion page that was presented in the privacy policy? [Yes; No, it's a different data deletion page; There was no data deletion choice presented in the privacy policy; Other (please specify)]

Logic: The following four questions are displayed if Q76 is not "Yes"

Step 14: Lastly, look through the main levels of the account settings for other types of user choices. Click links which seem to indicate user choice or preferences.

- 81. Did you find any other opt-outs in the account settings? [Yes, No]
- 77. According to the information provided, what actions can users perform related to data deletion? [Delete their account permanently, Suspend/deactivate their account (data will not be permanently deleted right away), Choose specific types of data to be deleted from their account, Not specified, Other (please specify)]
- 78. Please copy and paste the specific types of data it indicates. Use ";" to separate multiple items.
- 79. According to the information provided, does the website suspend or deactivate your account before deleting it? [Yes, there's information that says your account will be suspended; No, there's information that says your account will be deleted after a certain amount of time; Not specified within the account settings; Other (please specify)]
- 80. According to the privacy policy, after how long will the data be permanently deleted? [Not specified, Immediately, One week, 30 days, 60 days, 90 days, 6 months, Other (please specify)]
- 82. What other things can users opt out from in the account settings? [Device info; All first-party cookies; Location history; Profile activities/inferred interests; Sharing with third parties; Google Analytics; Other (please specify); None of the above]

“It’s a scavenger hunt”: Usability of Websites’ Opt-Out and Data Deletion Choices

Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou[†],
Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub[†]
Carnegie Mellon University & [†]University of Michigan
{htq, spearman, jiaminw, acquisti, lorrie, ns1i}@andrew.cmu.edu
{yixinz, fschaub}@umich.edu

ABSTRACT

We conducted an in-lab user study with 24 participants to explore the usefulness and usability of privacy choices offered by websites. Participants were asked to find and use choices related to email marketing, targeted advertising, or data deletion on a set of nine websites that differed in terms of where and how these choices were presented. They struggled with several aspects of the interaction, such as selecting the correct page from a site’s navigation menu and understanding what information to include in written opt-out requests. Participants found mechanisms located in account settings pages easier to use than options contained in privacy policies, but many still consulted help pages or sent email to request assistance. Our findings indicate that, despite their prevalence, privacy choices like those examined in this study are difficult for consumers to exercise in practice. We provide design and policy recommendations for making these website opt-out and deletion choices more useful and usable for consumers.

Author Keywords

Privacy; usability; privacy controls; email marketing; targeted advertising; data deletion.

CCS Concepts

•Security and privacy → Usability in security and privacy; Privacy protections; •Human-centered computing → Empirical studies in HCI; Empirical studies in interaction design; •Social and professional topics → Privacy policies;

INTRODUCTION

An expanding body of privacy regulations requires websites and online services to present users with notices and choices regarding the usage of their data. These regulations aim to provide transparency about data processing policies and give users access and control over their own data. Some regulations — such as the General Data Protection Regulation

(GDPR) and a few US laws — include specific usability requirements [3, 7, 40]. In part due to these regulations, privacy choices now seem to be ubiquitous on websites. Particularly common are opt-outs for email communications or targeted ads, options for data deletion, and controls and consent for use of cookies [15].

However, availability does not imply usability, leaving open the question of whether these controls are actually useful to consumers. We contribute a holistic usability evaluation of the end-to-end interaction required to use common implementations of these privacy choices. Past work has found various usability problems with such controls, particularly in tools for limiting targeted advertising (e.g., [12, 21]). We expand on that work by exploring the usability of websites’ own opt-outs for targeted ads. Furthermore, we examine choices beyond those related to advertising, providing insight into the usability of email marketing and data deletion choices required by the CAN-SPAM Act and GDPR, respectively.

We conducted an in-lab usability study with 24 participants. Participants were first asked about their expectations regarding websites’ data practices and privacy controls. They completed two tasks that were representative of common practices for offering privacy choices, as identified by prior work [15]. Tasks differed by the choice type (opting out of email communication, opting out of targeted ads, or requesting data deletion), choice location (account settings, privacy policy), and mechanism type (described in policy text, link from policy text).

We find that despite general awareness of deletion mechanisms and opt-outs for advertising and email, participants were skeptical of the effectiveness of controls provided by websites. On the nine websites studied, participants struggled most with discovering and recognizing pages with opt-out information and resorted to consulting help pages or contacting the website. Participants also expressed desire for additional controls over data sharing and deletion. Our findings suggest several implications applicable to websites similar to those in this study for making these online opt-out and deletion choices more usable and useful to consumers.

BACKGROUND & RELATED WORK

We first summarize legislation and self-regulatory industry guidelines relevant to controls for email marketing, targeted advertising, and data deletion. We then discuss prior studies on the usability of privacy controls.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author(s).
CHI '20, April 25–30, 2020, Honolulu, HI, USA.
© 2020 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6708-0/20/04.
<http://dx.doi.org/10.1145/3313831.3376511>

Regulatory Background

The European Union's General Data Protection Regulation (GDPR) requires websites to provide several types of privacy choices for European consumers and places a special emphasis on the usability of these choices. Relevant user rights under the GDPR include the "right to object" (Art. 21) to the use of data for direct marketing purposes and the requirement for clear affirmative consent to targeted advertising (Art. 4). Such consent in practice is often implemented by cookie consent banners [4]. Moreover, the GDPR grants a "right to be forgotten," allowing consumers to request data processors to delete their personal data (Art. 17) [8].

While the United States does not have a single comprehensive privacy law, several sectoral laws pertain to the privacy controls we examined in our study. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act requires companies to comply with consumers' wishes to opt out of receiving marketing emails, and provide a clear explanation for how to use the opt-out [10]. Other laws only apply to specific populations. For example, the Children's Online Privacy Protection Act of 1998 (COPPA) requires companies that collect data from children under 13 to honor parental requests to stop further data collection and delete already-collected data [11]. Effective in 2020, the California Consumer Privacy Act (CCPA) provides California residents rights to opt out of sales of their personal data for marketing purposes and, under certain circumstances, request deletion [3, 28].

Advertising industry organizations such as the Network Advertising Initiative (NAI), Digital Advertising Alliance (DAA), and Interactive Advertising Bureau Europe (IAB Europe) have adopted self-regulatory requirements for their online advertising practices [5, 17, 30]. Specifically, members of the DAA must provide consumers the choice to opt out of tracking-based targeted advertising [5]. In light of recent GDPR requirements, the IAB Europe also developed new guidelines for member advertisers related to transparency and consent [18].

Design of Privacy Choices

An empirical analysis of controls for email marketing, targeted advertising, and data deletion conducted by Habib et al. found that privacy choices are often presented through websites' user account settings and privacy policies. However, the terminology used in privacy policies to present these choices is inconsistent across websites, and quite often choices are not adequately described [15]. This has negative usability implications, as privacy policies still suffer from poor readability and consumers rarely read them [9]. Further exasperating this usability issue is the potential use of dark patterns and default settings, which could nudge users away from more privacy protective options [1, 13, 34, 43]. Gray et al. found that users are more likely to agree to the default option because of a belief that the product has their best interest in mind, which may not be the case with respect to data practices and privacy and could lead to unintended consequences [14].

While the goal of the GDPR is to empower consumers to have greater control over their personal data, Sanchez-Rola et al. found that numerous websites in the sample they analyzed

presented misleading information about choices, and few websites provided opt-outs for ad tracking that were easy to find or effective [37]. The GDPR also led to an increase in the display of cookie consent banners, but common implementations suffer from functional and usability issues [4]. Utz et al. found that consumers often clicked cookie consents out of habit, or believed that the website would not work absent a click on the consent box [42]. On the other hand, with the implementation of the GDPR, there is also some evidence that companies are shifting towards better practices. A study by Linden et al. suggests that the GDPR was a major driving force towards significant improvements in the presentation of privacy policies inside and outside of the EU [22].

Our study expands upon this prior work by examining user expectations for privacy choices and evaluating current practices for offering choices against these expectations. It highlights additional usability issues with the design of privacy choices that make them difficult for people to use and understand.

Usability of Privacy Choices

We next present prior work examining the usability of the privacy choices that were the focus of this study: email marketing, targeted advertising, and data deletion.

Email Marketing Opt-Outs

In addition to the risk of legal penalties, businesses may also risk losing customers by using poor practices in email unsubscribe processes. Results from a study of marketing unsubscribe choices by the Nielsen-Norman group indicate that users may become annoyed with companies and report legitimate messages as spam if unsubscribe options are not clear. They recommend making unsubscribe links easy to notice and click or tap on a mobile device. They also suggest removing unnecessary feedback steps or confirmation messages and avoiding confusing checkboxes on unsubscribe pages [31].

The Internet Society's Online Trust Alliance (OTA) conducted an audit of 200 North American online retailers to assess compliance with best practices for email sign-up and unsubscribe experiences. While the vast majority of audited retailers had adopted best practices, the report highlighted room for improvement, particularly related to the visibility of opt-out links in emails. While 84% of retailer emails had clear and conspicuous unsubscribe links, a third presented the link in a smaller than recommended font size. Additionally, 29% of retailers had unsubscribe text that did not meet minimum W3C guidelines for contrast ratios, and 64% of retailers did not meet W3C's enhanced guidelines [35].

Our study provides additional insight into the usability of email opt-outs through an empirical user study and evaluates email controls other than unsubscribe links, such as those offered through account settings and privacy policies.

Targeted Advertising Opt-Outs

Prior work has shown that websites are non-compliant with self-regulatory guidelines for targeted advertising, resulting in limited transparency in opt-out choices for users [16, 20]. Opt-out tools developed by the advertising industry have also been found to be misunderstood by users. Ur et al. showed

that the DAA's AdChoices icon does not clearly communicate whether or not an ad is targeted [41]. Additionally, NAI's opt-out tool led users to believe incorrectly that they were opting out of all data collection [26]. Furthermore, these opt-out tools rely on cookies, which can cause additional issues for users. For example, when users clear their cookies their opt-out preferences will also be removed in the process, which would require them to opt out again [25].

Browser extensions that block advertising trackers only partially resolve some of these issues. Studies have found that internet users download blocking extensions for a better browsing experience but still retain a limited understanding of online tracking [24, 38]. Pujol et al. found that many users use ad-blockers with default settings, which for some extensions might not actually block all web trackers [36]. This suggests that even with blocking extensions, people are not fully aware of the ad opt-out choices they can exercise online. While users state they want more control over tracking, they are reluctant to engage deeply with respective tools [27, 39].

Prior research has largely evaluated controls for targeted advertising on the basis of compliance with industry guidelines and users' perceptions of what they do, but has not holistically examined the end-to-end interaction required to use them. Our study provides additional insights by looking more deeply into how users discover targeted advertising controls, in the context of how they are commonly presented on websites.

Data Deletion Choices

Few studies have evaluated data deletion mechanisms, and thus there are few guidelines or best practices. Murillo et al.'s 2018 qualitative study examined user understanding of online data deletion and expiration. They found that most participants were aware of a "backend" to the data deletion process (versus having an understanding completely based on user interface components such as delete buttons and trash icons), and they suggested that information about data deletion should use this understanding to explain technical constraints of data deletion and to help users understand data retention periods. They also found that participants preferred to have context-dependent control over the expiration of their data, rather than just having a fixed chronological expiration period [29].

Recent evidence indicates that the GDPR has led to increased availability of deletion controls, which are often provided as instructions through a website's privacy policy for requesting deletion of personal data [13, 15]. The service JustDelete.me provides a database with ratings of the ease of deleting data from over 500 different websites, and compiles direct links to the deletion options on those sites. Nearly 40% of the websites listed in the database are rated as having "hard" or "impossible" deletion processes. However, this database does not provide analyses of the full user interaction required to delete data, nor does it publish its methodology for determining these ratings or suggest best practices for deletion interfaces [19].

In 2019, Habib et al. analyzed 150 English-language websites to assess the usability and interaction paths of data deletion mechanisms (as well as email and advertising opt-out mechanisms). While 74% of websites in their sample offered deletion

controls, only 27 included a direct link to a tool or request form; 81 offered instructions for a data deletion request rather than providing a simple tool or form. The types of deletion and expiration options were not consistent from website to website, and the time frame in which data deletion would occur was often ambiguous. Many actions, including form fields and extraneous confirmations, were sometimes required in order to delete data. For example, 38 user actions — including filling out a form with 22 checkboxes — were required to request data deletion from the New York Times [15].

While prior work has studied users' mental models of data deletion through interviews [29], prior usability evaluations of deletion controls have relied on analysis by usability experts [15, 19]. Our study builds on this work with a user study that confirms reported usability issues and uncovers others.

STUDY DESIGN

We conducted a lab study with 24 participants. In this section we describe our study design and data analysis approach.

Study Session Components

Each lab session consisted of an interview portion followed by a set of tasks conducted on a lab computer. Participants were also asked follow-up questions after completing each task.

Interview

The first portion of the study session, a semi-structured interview, had a median length of 11 minutes (min: 5 minutes, max: 22 minutes). First, we asked participants what types of data they thought websites collected about them and how they thought it was used. Next we asked participants what types of controls they expected to have over how websites could use their data, as well as where they expected to be able to find these controls. To learn more about expectations related to email marketing, targeted advertising, and data deletion specifically, we asked participants to recall a recent time when they received a marketing email, saw a targeted ad, and provided a website with personal information. For each, we followed up with questions about what types of control they thought were available, and how they would attempt to exercise that control.

Task Selection

In the second portion of the study session, we asked each participant to complete two opt-out tasks on a lab computer. In each task, participants were asked to use a privacy choice on a website while thinking aloud. Each privacy choice task was one of the following: opting out of email newsletters from a website, opting out of targeted advertising on a website, or requesting deletion of personal information from a website. Although other privacy choices exist, we wanted to examine the usability of a set of choices over different types of data handling practices. Additionally, the choices selected are prevalent in the current online ecosystem and fall under legal or other regulatory requirements.

In prior work, we reviewed controls for email marketing, targeted advertising, and data deletion on 150 websites and found that these choices are most commonly presented using one of three patterns: a user account setting, a link from the privacy policy, or text instructions in the privacy policy [15]. To

Website Name	Task Type	PP AS	# Actions	Mechanism
majorgeeks.com	email	AS	9	checkbox
foodandwine.com	email	PP	5	link to email options
internshala.com	email	PP	9	text, refer to emails
wordpress.com	ads	AS	9	toggle option
colorado.edu	ads	PP	16	links to opt-out tools
coinmarketcap.com	ads	PP	10	text, delete cookies
phys.org	deletion	AS	9	delete account
nytimes.com	deletion	PP	46	link to request form
runescape.com	deletion	PP	9	text, email request

Table 1. The websites used for email opt-out, targeted advertising opt-out, and date deletion tasks and their associated mechanisms in the privacy policy (PP) and account settings (AS), as well as the minimum number of user actions required to exercise each control.

identify specific tasks for this user study, we examined the collected empirical data and looked for websites that used just one of the three patterns (some websites used more than one pattern, e.g., both a user account setting and privacy policy link). For each of the *task types*, we selected three websites that followed these patterns, resulting in a set of nine websites. The websites selected and their choice mechanisms in the privacy policy or user account settings are presented in Table 1.

To minimize learning effects and prevent fatigue, we counter-balanced and stratified tasks such that each participant completed two different task types. One task was selected to be on a website with an account settings mechanism and the other task on a website with a privacy policy mechanism, allowing us to examine the usability of the most common practices used by websites. This resulted in 12 possible groupings of the websites selected for the study. We recruited 24 participants and assigned a pair of participants to each grouping, with each member of the pair performing the tasks in the inverse order.

Task Introduction

Prior to each study session, researchers opened a new window in Google Chrome’s Incognito mode and logged into a Gmail account created for the study. Before being given their first task, participants were told that they could use this Gmail account and could search online for any information that they needed to complete the task. Participants were also notified that, if applicable, they could assume they had user accounts on the websites they would visit for the study tasks. Participants were not required to use their own credentials or personal information for any of the tasks, and instead were provided with credentials created for the study through printed index cards when reaching the log-in step on the website.

We described the email opt-out, targeted advertising opt-out, and deletion tasks to participants as the following scenarios:

You just got the tenth update email from [website] today, and now you want to stop receiving them.

You’ve been seeing advertisements on [website] for a pair of shoes that you searched for last month, and now you want to stop seeing them.

You’re uncomfortable with [website] keeping a record of your location, and want to remove all of your data from the company’s databases.

After being read the appropriate scenario, participants were instructed to open a new browser tab or proceed as they would at home while thinking aloud.

Task Follow-Up

After each task, we asked a set of follow-up questions regarding the participant’s experience with the task and their understanding of what effects their actions would have. We also asked about their past experiences with similar tasks and their familiarity with the website used in the task.

After participants completed both tasks and the task follow-up questions, we asked them which task they found easier, and why. We also asked about their past choices to use opt-out mechanisms or privacy controls on websites. Lastly, we inquired as to whether they wished websites offered any additional controls related to privacy or personal data and what they thought they should look like.

Data Collection

One researcher moderated all participant sessions. A second researcher attended each session to take notes. At the beginning of their session, participants completed a consent form that described the nature of the interview and tasks and notified participants that audio and screen recordings would be captured. We audio-recorded participants’ responses to interview questions, comments and questions during the computer tasks, and responses to follow-up questions after the computer tasks. Participants’ actions during the computer tasks were screen-recorded. This study was approved by the Institutional Review Boards (IRB) at Carnegie Mellon University and the University of Michigan.

The 24 participants were recruited locally in Pittsburgh, Pennsylvania using Craigslist, Reddit, and a university subject pool. In recruitment posts, potential participants were invited to complete a screening survey with questions about demographics, as well as engagement in four common privacy practices selected from a Pew Research Center survey [23]. A sample of participants — diverse in gender, age, and educational attainment — was selected from among the respondents. Those who completed the in-lab study session were compensated with a \$20 Amazon gift credit. The study sessions lasted a median of 50 minutes (min: 30 minutes, max: 78 minutes). The large variance in session duration was related to how fast participants were able to complete their tasks. While all participants attempted their tasks, those who stated they did not know what to do next or still had not completed the task after eight minutes were given a hint to log in or look for a “privacy-related page” (depending on the task). This threshold of eight minutes was determined through pilot sessions. Any assistance provided was noted and incorporated into our analysis.

Data Analysis

Interview recordings were transcribed using an automated transcription service (temi.com), and a researcher then corrected errors in the transcripts. The use of a third-party transcription service was IRB-approved, and participants consented to the sharing of recordings with a third-party service. We took extra measures to preserve participants’ privacy prior to uploading the recordings by removing any personally identifying

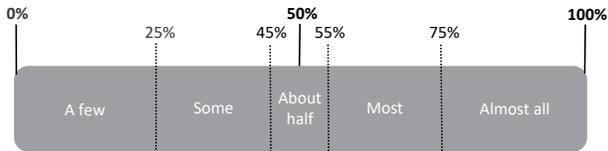


Figure 1. Terminology used to present relative frequency of themes.

details, such as name and address, that a small number of our participants revealed during their interview. We conducted inductive coding on the interview transcripts. To develop an initial codebook, one researcher performed open coding to identify themes and merged common codes as needed. Two researchers then collaboratively revised the codebook after individually coding a random sample of six interviews using the initial iteration of the codebook and reviewing all disagreements in their coding. After coming to an agreement on the codebook, the remainder of the interviews were double-coded. Any disagreements were again reviewed and reconciled.

We created an analysis template to systematically count the interactions and errors made during the tasks. One researcher reviewed all screen recordings of the session tasks along with any researcher notes from the session to create initial counts of interactions and errors. Another researcher then reviewed and confirmed the interactions recorded.

We organized our findings according to the User Action Framework, which offers a systematic framework for assessing and reporting usability data. Within this framework, Andre et al. [2] adapted Norman’s theory of human-computer interaction [32] and discuss user interaction in terms of four cyclic phases: high-level planning (“users determine what to do”), translation (“users determine how to do it”), physical action (“users do the physical actions they planned”), and assessment (“users assess the outcome of their actions”). We previously applied this framework to online privacy choices in our empirical analysis of opt-out and data deletion actions across websites, and mapped these phases of the interaction to *finding*, *learning*, *using*, and *understanding* privacy choice mechanisms [15]. Here we apply the same framework to the actions we observed in the lab.

As our study was primarily qualitative, we do not report exact numbers when presenting most of our study findings. However, following recent qualitative work at CHI [6], we adopted the terminology presented in Figure 1 to provide a relative sense of frequency of major themes.

Limitations

The exploratory nature of this study provides insights into possible usability issues with common practices used to provide privacy choices, but cannot provide quantitative claims about how frequently these issues may occur in the real world. Similarly, our limited sample size of 24 participants, though diverse, was not representative of all internet users, and likely over-represented technically savvy users. Thus the frequency of issues reported by our participants may not reflect the frequency with which these issues would be encountered by a general population. However, it is unlikely that less technically

savvy users would face fewer issues when opting out or deleting their data. As such, the issues and opinions highlighted only represent a subset of all possible ones.

While our sample of nine websites was representative of the common practices websites use to provide privacy choices, it is not representative of all types or categories of websites that exist. Our results may not generalize to other types of websites, particularly those that are more complex than those included in our sample and offer multiple products or services. Additionally, design variations and specific peculiarities of each website may have impacted the difficulty of exercising the privacy choices present and thus participants’ opinions. However, this was a deliberate trade-off as using live websites allowed us to gain insight into the usability of real-world privacy choices. We note specific features that seemed particularly detrimental or helpful when exercising privacy controls.

While our study was designed to mitigate learning effects, it is still possible that participants used knowledge acquired in their first task to complete their second task. Similarly, while we avoided directly mentioning “privacy” or “security” during the pre-task interview (unless a participant brought up the topic), the questions may have biased participants to think more about privacy and security than they otherwise would have.

PARTICIPANTS

Table 2 provides a summary of participant demographics, as well as which tasks participants were assigned. In our sample, 13 participants identified as female and 11 as male. Our sample had a wide distribution of ages, but skewed towards higher levels of educational attainment. Six participants reported having an education in or working in computer science, computer engineering, or IT. In their responses to the screening survey, all 24 participants reported to have cleared cookies or browsing history, 22 had refused to provide information about themselves that was not relevant to a transaction, 13 had used a search engine that does not keep track of search history, and 10 added a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger. This distribution is somewhat higher than that found by Pew [23], suggesting our sample may be more privacy-aware than the general public. Almost all participants reported having prior experience with controls for email marketing, and most had prior experiences with advertising and deletion controls.

RESULTS

We next present our findings structured around the four stages of the interaction cycle: finding, learning, using, and understanding privacy choice mechanisms. We highlight participants’ expectations, actual performance in session tasks, as well as website practices that make exercising privacy choices more difficult for users and those that make it easier.

Planning: Finding Privacy Choices

Participants expected to find privacy choices within the context of how a website uses their data (for example, unsubscribe links within emails) or on a user account settings page. The presence of multiple paths to a privacy control made the control easier to find.

ID	Gender	Age	Education	Technical	Task 1	Task 2
P1	F	35-44	Professional		majorgeeks	runescape
P2	F	18-24	Bachelors		wordpress	internshala
P3	F	25-34	Some college		wordpress	foodandwine
P4	M	55-64	Bachelors		wordpress	nytimes
P5	F	45-54	Bachelors		wordpress	runescape
P6	F	25-34	Masters		phys	internshala
P7	F	45-54	Associates		phys	foodandwine
P8	F	25-34	Bachelors		phys	coinmarketcap
P9	F	25-34	Bachelors		phys	colorado
P10	M	25-34	Masters	X	colorado	majorgeeks
P11	M	55-64	Masters		nytimes	majorgeeks
P12	F	18-24	Associates		internshala	wordpress
P13	M	35-44	Some college	X	foodandwine	wordpress
P14	F	18-24	Bachelors		nytimes	wordpress
P15	M	18-24	Bachelors		runescape	wordpress
P16	F	55-64	Bachelors	X	foodandwine	phys
P17	M	45-54	Associates	X	coinmarketcap	phys
P18	M	55-64	High school		colorado	phys
P19	F	55-64	Masters		majorgeeks	coinmarketcap
P20	M	35-44	Associates	X	majorgeeks	colorado
P21	F	35-44	Masters		majorgeeks	nytimes
P22	M	25-34	Bachelors		coinmarketcap	majorgeeks
P23	M	18-24	Masters		internshala	phys
P24	M	25-34	Bachelors	X	runescape	majorgeeks

Table 2. Participant demographics (gender, age, education, technical background) and task assignments.

Expectations are dependent on choice type

In response to pre-task questions, some participants mentioned expecting to find data-use controls in the account settings or on a privacy settings page. A few participants mentioned consent dialogues, either through the browser or the website. Additionally, a few participants described browser settings or functions, such as private browsing and plugins.

Participants had similar responses when describing where they would like privacy controls to be placed. Half of the participants suggested that controls should be placed within a website’s account settings. Some preferred to see privacy controls in context on the website (e.g., where data is collected). Other suggestions provided by participants included being able to email a company with requests and receiving monthly digest emails summarizing the data the website has about them.

When asked about email marketing controls, almost all participants mentioned unsubscribe links within emails. Some also described more granular controls, such as the ability to select which marketing messages to receive or to change the frequency of emails through website account settings. Some described other control mechanisms, such as contacting the website and using unsubscribe features built into email clients.

To control the display of targeted advertising, about half the participants mentioned privacy enhancing strategies, such as using ad-blocking extensions, clearing the browser history, using private browsing mode, changing browser settings, or using a privacy-protective search engine. A few participants mentioned being able to find controls by interacting with the corner of an advertisement (likely referring to the DAA’s Ad-Choices icon or ad controls provided by social media sites). Only a few participants mentioned controls for advertising being available in the account settings. A few also mentioned avoiding clicking on ads as a type of control.

Most participants expected deletion controls to be available in the account settings, and some believed that deletion could be achieved by contacting the website. Only a few participants

mentioned finding deletion controls elsewhere on the website, such as in a frequently-asked-questions page.

Participants’ initial strategies varied by choice type

Most of the 16 participants assigned to an email opt-out task first looked for or used an unsubscribe link in an email sent by the website, which could be found in the provided Gmail account. Almost all participants reported using such links prior to the study. A few had other initial strategies for finding unsubscribe mechanisms, such as using the search feature of the browser to find the term “unsubscribe” on the home page or the search feature of the website to find the privacy policy.

Participants used a variety of strategies for completing their targeted advertising opt-out task, some of which were more effective than others. Some first went to the account settings, while only a few first looked in the privacy policy. A few explained that they would try to find an ad on the website and look for an icon leading to opt-out options. A few went into the browser settings to look for advertising-related options, while a few others immediately resorted to emailing the website for help. As P18 reasoned, “Well, if they’re not able to help then they would respond back and say here is the correct way to opt out of what you’re looking for.” A few participants looked for opt-out choices on other pages, such as the website’s cookie policy, terms of service, and frequently-asked-questions page.

Participants had a more uniform set of strategies for deletion mechanisms. Most immediately logged into the website. A few resorted to frequently-asked-questions pages or contacting the website. Finally, a few participants looked for account-related information in registration emails from the website.

Policy and settings mechanisms required assistance

Almost all participants required assistance finding the account setting or privacy policy mechanism related to their study task. On the three websites that had privacy choices in account settings, some were able to use the mechanism on their own after being prompted to log into the website, but a few needed further guidance to look within the account settings to complete the task. P6, who was unable to find the advertising opt-out on **wordpress.com** described the process: “It’s what I call a scavenger hunt. I’ve gone all throughout this website, apparently a legitimate website, but I still can’t do what I really like to do.” On the six websites where the privacy choices were in the privacy policy, some were able to find the privacy choice text or link without guidance (however P10 admitted they were prompted to think about privacy because of the pre-task interview). A few were able to use the choice mechanism after they were given the hint to look for a privacy-related page, while a few others did not initially see the control in the policy and required prompting to look further.

Poor labels cause confusion

On two of the websites, there were multiple pages that had labels with words that were related to what the task was. For example, some participants assigned to opt out of email marketing from **majorgeeks.com** went to a different settings page called “alert preferences” that included settings related to notifications received while on the website. The correct setting



Figure 2. Screenshot of settings menu on majorgeeks.com where participants had difficulty finding the correct path to e-mail opt-outs.

could be found under the “privacy” or “contact details” settings pages. However, as seen in Figure 2, these options were presented in a list with no descriptions. Similar confusion occurred on coinmarketcap.com where a few participants assigned to find controls related to targeted advertising went to a page linked from the homepage called “advertisers” with information for companies that wished to place ads on the site. This suggests that more descriptive labels on these websites would help users find choice mechanisms more easily.

Multiple paths made choices easier to find

On some websites, there were multiple paths to the same choice mechanism, which made them easier to find. All participants assigned to request data deletion from nytimes.com first visited the account settings, where they found a link to the privacy policy, which in turn contained a link to the request form. Similarly, most participants assigned to request data deletion from runescape.com used the site’s search feature or looked through its support pages and found a page titled “Your Personal Data Rights,” which provided a summary of the same information provided in the privacy policy. However, one additional location where participants expected an opt-out choice for email marketing was on the page to subscribe to emails. All four participants assigned to find the opt-out link in foodandwine.com’s privacy policy clicked on the prominent “subscribe” button on the homepage and expected to find a means to unsubscribe.

Translation: Learning Privacy Choices

Participants had clear expectations about what choices available to them should do. We also observed several design decisions made by websites that impacted participants’ comprehension of these choices.

Participants desired controls over data sharing and deletion

Participants demonstrated incomplete mental models of the choices that were provided to them, especially when describing controls related to how websites can use collected data in the abstract. The only website-offered controls that were mentioned by multiple participants were cookie consent notices and security controls, such as encryption or multi-factor authentication. A few participants mentioned withholding information about themselves when using a website or avoiding

using a website entirely. However, a few participants discussed deletion controls prior to being prompted.

Participants’ understanding of website-provided controls appeared more concrete when asked about specific practices, such as email marketing, targeted advertising, and data deletion. As mentioned earlier, nearly all reported that they had used unsubscribe links within emails. Related to advertising, some participants expected to be able to report a particular advertisement as irrelevant. Half of the participants who mentioned this type of control also mentioned seeing such a control on a social media website, such as Facebook or Twitter. Only a few expected to be able to opt-out of targeted advertising entirely. When asked about choices related to data deletion, some were unaware of deletion controls offered by websites, but about half expected to be able to delete data from their profile and some mentioned being able to delete their entire account. Nearly all participants who mentioned a deletion mechanism stated that they had used such controls in the past.

When asked about privacy controls they wished websites offered, most participants mentioned controls for data sharing and deletion. As P11 stated, “*Well in the ideal world, you should be able to tell the website, look, I’m giving you this information, but don’t share it.*” A few mentioned wanting to tell websites to not save their information, while a few others desired greater controls over content that is displayed to them, such as recommended articles. More broadly, a few participants expressed a desire for greater transparency about data sharing or existing controls. However, a few others stated that they were satisfied with their current privacy options or could not articulate additional desired control mechanisms.

Formatting and text cause confusion

Another usability issue that made it difficult for participants to interpret choices was poor formatting and explanatory text. Most participants trying to find information about opt-outs for advertising in coinmarketcap.com’s privacy policy clicked on the link to install the Google Analytics opt-out browser extension, likely due to the placement of a link in policy text referring to advertisers and the use of cookies. However, the opt-out extension only opts users out of Google’s tracking for analytics purposes, and not advertising. Similarly, most participants assigned to runescape.com found a page related to data rights, but had difficulty figuring out how to actually request deletion because of the page’s format. As seen in Figure 3, removing your personal data appears to be a clickable option. However this is not the case and most were confused about why nothing appeared to happen. The text description provided after a list of data rights directs users to complete a subject access request form, labelled as “Make a Subject Access Request,” which is linked after a button labelled “Fix it Fast: Account Settings.” Most participants who saw this page incorrectly clicked on the account settings link instead of requesting deletion through emailing the contact provided on the page or the request form, as instructed. The placement of these two links made it unclear which privacy rights listed on the page could be accomplished through each mechanism.¹

¹This page on runescape.com was updated after our study. The new version partially addresses these issues by reducing the page’s



Figure 3. List of data rights available on runescape.com which misleadingly seem clickable.

Conversely, colorado.edu's privacy policy contained links to the three advertising opt-out tools in a single paragraph, which led participants to at least see all three tools (even if none actually selected all three, as discussed in the next subsection).

On phys.org a clear "Manage account" button visible on the landing page of the account settings conveyed the correct interaction path to almost all participants assigned to the website. However, some of the participants who clicked this button and saw the setting to delete the account were unsure whether that mechanism would also delete their data, and navigated away from the page to look for other options. A statement indicating that profile data will be erased permanently was not presented until after clicking the initial delete button. However, once participants saw this confirmation they were assured that the mechanism would accomplish their task.

Physical Action: Using Privacy Choices

Exercising privacy choices required a high level of effort from participants, as measured by the number of actions such as clicks, scrolls, and checkboxes in the interaction path of using a choice mechanism. Certain practices used by the websites in our sample made exercising choices more difficult.

High level of effort exerted in exercising policy choices

Figure 4 displays the number of user actions in participants' interaction path when using privacy choices located in the account settings and privacy policy. Using a choice mechanism in account settings resulted in an average of 26.1 user actions (min: 8, max: 43, sd: 11.5). Interactions using links in the privacy policy had 37.5 actions (min: 11, max: 59, sd: 15.2), on average, and those with text instructions in the policy had 57.6 (min: 18, max: 87, sd: 27.5). While policy links took participants exactly where they needed to go, text instructions were vague and required extra effort to figure out what to do. Furthermore, participants took many more steps than text. However, it is still unclear which privacy rights listed can be accomplished by the two mechanisms shown.

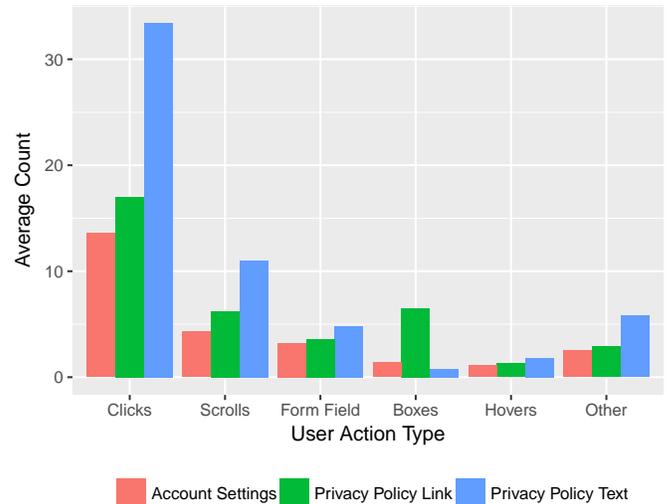


Figure 4. Number of clicks, scrolls, form fields, check boxes, hovers, and other user actions, averaged over all websites, in the participants' interaction with account settings and policy choices.

the shortest, ideal path for completing a task. The shortest interaction path for account settings mechanisms would have taken 9 total actions averaged over the three websites, while policy link choices needed 22.3, and policy text required 9.3.

Most participants who used the account settings mechanisms on wordpress.com or phys.org said that they were easy to use because of the simplicity of the setting. For example, P6 described the account deletion process on phys.org: "It said delete my account which was pretty clear. And then there was this other page that like made it very clear that that's what was going to happen." Some noted that these mechanisms were easy to find. A few appreciated that, unlike another mechanism they used, the account settings option would be applied right away and did not require a response from the website. Nearly all participants assigned to opt out of emails from majorgeeks.com also found the mechanism straightforward or easy to use, but most found the setting hard to find.

Participants who were assigned to tasks with privacy choice links or text instructions in the website's privacy policy explicitly mentioned that they found these mechanisms hard to find or that finding them required too much reading. Reactions to the data deletion request form on nytimes.com were mixed. Most participants disliked being presented with many similar-seeming options related to data processing, only being able to submit one request type at a time, or having to manually select 22 services from a list. However, others reported that the policy was easy to find through the account settings and the form was straightforward to use.

Unsubscribe links within emails were also considered straightforward to find and use. Participants highlighted user-friendly features these pages that they encountered previously or during the study. These included opt-outs that were automatically applied without extra confirmation or entry of their email address, as well as interfaces that allowed users to select emails

from the website they would like to continue to receive (as long as a button to opt-out of all emails was visibly present).

Choices require unnecessary user effort

Some practices used by websites for offering privacy choices place undue burden on users. An example is requiring users to submit written requests, a common practice websites use to offer data deletion [15]. Participants had difficulties articulating such requests. P4, who was trying to opt-out of targeted advertising on wordpress.com, drafted a message to customer service that asked “*How can I delete a specific webpage that is contacting me?*” Additionally, a few participants who wrote account deletion or unsubscribe requests did not include all the information the website would need to act on their request, such as the username or email address.

Another practice that complicates opt-out choices for users is offering multiple links to different opt-out tools. The privacy policy for colorado.edu contained links to advertising opt-out tools offered by the DAA, NAI, and Google. All participants assigned to this website visited only one or two of the three links. Participants had varying justifications for which links they clicked on. Half selected the DAA and NAI links because they (correctly) believed they would apply to multiple third-parties and not just Google. However, many entities participate in both industry opt-out programs, and participants may not have realized the overlap. Another explained that they chose to click on the Google advertising opt-out because they were already within Google’s ecosystem (i.e., using Google Chrome and Gmail) so they thought the opt-out would be more broadly applied, especially if they stayed logged into the Google account. Though Google owns the largest online advertising exchange, using an industry provided opt-out tool may have greater impact on limiting targeted ads.

Simple design flaws also place extra burden on users. For example, on majorgeeks.com when a user changes a setting it is not automatically saved; users have to press a “save” button at the bottom of the page. The website also does not provide a warning that there are unsaved changes. A few participants assigned to this website found the correct opt-out setting but did not press “save,” resulting in lost changes and the opt-out not being applied. This is an example of a post-completion error [33]. In contrast, a warning reminded a few participants assigned to wordpress.com to save their changed settings.

Assessment: Understanding Privacy Choices

Participants expressed skepticism that the privacy choices they use will actually be honored by websites. Websites were also unclear about what happens when such controls are used.

Skepticism of privacy choice effectiveness

During the pre-task interview, participants expressed doubts that data-related controls companies offered actually were effective. A few thought that there was nothing they could do to control ads, or were skeptical that available control mechanisms changed which ads were displayed. As P16 explained, “*It’s like the door open/close on the elevator. It’s just there to make you feel like you have some power. But I really don’t think it does anything.*” Others assumed data-sharing agreements between companies precluded opt-outs. P12 explained,

“I think it would be really difficult to like kind of untether them from each other cause I know they have a lot of agreements with each other and stuff like that.” Some expressed skepticism that their data would actually be permanently deleted by a company when requested. As P6 stated, “*I think that I could like go through the motions of deleting the information, but I feel like it might still be there even if I tried to delete it.*”

We also noted that skepticism of deletion choices persisted even after participants used deletion mechanisms in the study. A few participants assigned to phys.org believed they were simply deactivating their account and that their account data would not actually be deleted by the company. A few others assigned to nytimes.com or runescape.com were unsure whether or not their data would be fully deleted.

We observed that participants had more confidence in the mechanisms they used to opt-out of email marketing, due in part to prior experience. Almost all participants who used an email opt-out believed that they would eventually stop receiving emails from which they opted out, even if it takes a few days. A few mentioned they might receive a final email to confirm their unsubscribe request.

Confusion about scope of targeted advertising opt-outs

Most participants assigned to use an advertising opt-out had misconceptions about whether the mechanism they used would be effective across different browsers or devices. Some who used cookie based opt-outs on coinmarketcap.com or colorado.edu were unsure or had misconceptions about whether they would continue seeing targeted ads. Most misconceptions were related to inaccurate mental models of how cookies were stored, with some believing that they were synced to a user’s Google profile. Thus they believed that any changes to cookies made using Chrome on a computer would prevent them from seeing targeted ads when they used Chrome on their phone.

DISCUSSION

We conducted an in-lab study with 24 participants to explore the usability and usefulness of privacy controls. Our results highlight several design and policy implications for how websites, particularly those that offer a small number of privacy choices such as those in our sample, should present controls for email marketing, advertising, and deletion. However, further study is needed before these initial findings can be translated to broader policy or design recommendations.

Design Implications

We noted several design decisions that made completing the privacy choice tasks particularly difficult, as well as some that seemed to aid participants. Our findings are especially relevant to controls in user account settings or privacy policies.

Provide unified settings in a standard location

Unifying privacy choices into a single, standard location (perhaps in the form of a dashboard) would likely make these controls easier for users to find. Some participants recognized that many websites have controls in account settings pages and looked for controls there. If the practice of putting privacy choices in account settings was more widely adopted and promoted, it is likely that most users would learn to look there.

However, privacy controls for which a login is not essential should also be available without requiring users to log in or even to have an account.

Privacy controls could also be implemented as an interface within web browsers, which in turn could convey users' choice information to websites in a computer-readable format. This could allow for opting out once for all websites (the idea behind the Do Not Track mechanism), or for all websites that meet certain criteria. It could also save users the effort of finding choice mechanisms on websites and instead allow them to go to the choice menu in their web browser, where they would be provided with available choices that could be exercised through the standard interface.

Supplement with additional paths and in-place controls

Even after unifying choices in one place, websites should still offer multiple paths to those controls so that they are easy to find. Links to privacy controls should be placed anywhere users might look, such as the account settings, privacy policy, and website help pages. For example, all participants assigned to the nytimes.com reached the deletion request form in the privacy policy through the account settings, not the link in the website footer mandated by the California Online Privacy Protection Act (CalOPPA). Websites should ensure that if they have multiple links or mechanisms they are consistent with each other and lead to the same results.

Control mechanisms that are offered within the context of how data is used by the website can also supplement unified privacy dashboards. With email marketing, participants in our study were generally aware of unsubscribe links in emails and thought they were easy to find. Similarly, a few participants recalled the ability to control targeted ads on a website by interacting with the corner of an ad.

Reduce effort required to understand and use choice

Websites in our study imposed much of the effort required to exercise privacy choices onto users. It was up to users to distinguish between multiple targeted advertising opt-out tools and figure out how to articulate written deletion requests. For these choices to actually be useful, websites need to place more effort into packaging them into simple settings offered through the website. The mechanisms participants favored the most in our study were toggles or clearly-labelled buttons offered in the account settings. Such settings could automatically place opt-out requests through commonly used industry tools such as those offered by the DAA and NAI, or trigger database queries to remove a user's personal information.

How privacy controls are labelled and organized in a unified privacy dashboard will impact their usability. Our study highlighted that imprecise navigation labels may confuse users. Within a page, controls should be clearly organized and labelled. Websites should conduct user testing with the design of their particular privacy dashboard pages to ensure that people can find the information they need.

Bolster confidence that choices will be honored

Participants in our study were skeptical that privacy choices would actually be honored by websites. Better communication about what exactly a setting does also could help relieve

skepticism. For example, phys.org stated the time period after which account data would be deleted in the final step of the account deletion process. Websites should also provide confirmation that a choice has been applied after users complete the process. A confirmation message can be displayed within the website itself if the choice is immediately applied. For choices, such as email unsubscribes, that require time to process and complete, at minimum there should be a confirmation message that acknowledges the request and provides a clear estimate of how long it will take to honor the request. For requests, such as those for data deletion, that may take more time before the choice is fully applied, the website should also send a confirmation email.

Public Policy Implications

The recent enactment of comprehensive privacy legislation, such as the GDPR and CCPA, require companies to not only offer privacy choices, but also make them usable. Prior laws, such as the CAN-SPAM Act, included requirements for privacy mechanisms to be clear and conspicuous. Our results indicate that website privacy choices similar to those in our study remain difficult for users to find and use, but that some of these usability requirements are having an impact.

We observed that unsubscribe links within emails had better usability relative to the user account and privacy policy mechanisms we studied. This is likely an effect of CAN-SPAM Act requirements. From our study, it is apparent that unsubscribe links are widely used and that, over time, people have learned to expect these links in the marketing emails they receive. For other regulation to have similar impact, design guidelines for how websites should present privacy choices may be helpful. Guidance on where and how privacy controls should be presented will likely lead to less variation among websites and could allow users to develop consistent expectations. Moreover, future regulation should incorporate the results of usability studies to inform these design guidelines or could require websites to conduct user testing to ensure that choices are useful and usable for consumers.

CONCLUSION

We conducted a 24-participant in-lab usability evaluation of privacy controls related to email marketing, targeted advertising, and data deletion. Our findings highlight the need to better align the location and functionality of choices to user expectations of where to find these choices and how to operate them. Additionally, simple interface changes, including better labeling and use of confirmation messaging, would make choices more useful and increase users' confidence in their effectiveness. Furthermore, the relative success of unsubscribe links mandated by the CAN-SPAM Act suggests that the standardization of choices through regulation could improve the usability of choices.

ACKNOWLEDGMENTS

This project is funded in part by the National Science Foundation (CNS-1330596, CNS-1330214), the Carnegie Corporation of New York, and Innovators Network Foundation. We wish to acknowledge all members of the Usable Privacy Policy Project (www.usableprivacy.org) for their contributions.

REFERENCES

- [1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, and others. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 44.
- [2] Terence S Andre, H Rex Hartson, Steven M Belz, and Faith A McCreary. 2001. The User Action Framework: A Reliable Foundation for Usability Engineering Support Tools. *International Journal of Human-Computer Studies* 54, 1 (2001), 107–136.
- [3] California State Legislature Website. 2018. SB-1121 California Consumer Privacy Act of 2018. (2018). https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.
- [4] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*.
- [5] Digital Advertising Alliance. 2009. Self-Regulatory Principles for Online Behavioral Advertising. (July 2009). <http://digitaladvertisingalliance.org/principles>.
- [6] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor Into IoT Device Purchase Behavior. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*.
- [7] European Commission. 2018a. Article 29 Data Protection Working Party. Guidelines on Transparency under regulation 2016/679. (2018). http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm.
- [8] European Commission. 2018b. EU Data Protection Rules. (2018). https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
- [9] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. 2017. Large-Scale Readability Analysis of Privacy Policies. In *Proceedings of the International Conference on Web Intelligence (WI)*. 18–25.
- [10] Federal Trade Commission. 2009. CAN-SPAM Act: A Compliance Guide for Business. (2009). <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>.
- [11] Federal Trade Commission. 2017. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. (2017). <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>.
- [12] Stacia Garlach and Daniel Suthers. 2018. 'I'm supposed to see that?' AdChoices Usability in the Mobile Environment. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*.
- [13] Global Privacy Enforcement Network. 2017. GPEN Sweep 2017: User Controls over Personal information. (2017). https://www.privacyenforcement.net/system/files/2017%20GPEN%20Sweep%20-%20International%20Report_0.pdf.
- [14] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*.
- [15] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.
- [16] Jovanni Hernandez, Akshay Jagadeesh, and Jonathan Mayer. 2011. Tracking the Trackers: The AdChoices Icon. (2011). <http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon>.
- [17] IAB Europe. 2011. EU Framework for Online Behavioural Advertising. (2011). https://www.edaa.eu/wp-content/uploads/2012/10/2013-11-11-IAB-Europe-OBA-Framework_.pdf.
- [18] IAB Europe. 2019. GDPR Transparency and Consent Framework. (2019). <https://iabtechlab.com/standards/gdpr-transparency-and-consent-framework/>.
- [19] JustDelete.me. 2019. A directory of direct links to delete your account from web services. (2019). <https://justdeleteme.xyz>.
- [20] Saranga Komanduri, Richard Shay, Greg Norcie, and Blase Ur. 2011. AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements. *A Journal of Law and Policy for the Information Society* 7 (2011).
- [21] Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012. What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.
- [22] Thomas Linden, Hamza Harkous, and Kassem Fawaz. 2018. The Privacy Policy Landscape After the GDPR. *arXiv:1809.08396* (2018).
- [23] Mary Madden and Lee Rainie. 2015. Americans' Attitudes About Privacy, Security and Surveillance. (2015).

- [24] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the use of browser-based blocking extensions to prevent online tracking. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.
- [25] Jonathan R Mayer and John C Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*.
- [26] Aleecia M McDonald and Lorrie Faith Cranor. 2010. Americans' Attitudes About Internet Behavioral Advertising Practices. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.
- [27] William Melicher, Mahmood Sharif, Joshua Tan, Lujio Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. 2016. (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies* 2016, 2 (2016), 135–154.
- [28] Michael Morgan, Daniel Gottlieb, Matthew Cin, Jonathan Ende, Amy Pimentel, and Li Wang. 2018. California Enacts a Groundbreaking New Privacy Law. (2018). <https://www.mwe.com/en/thought-leadership/publications/2018/06/california-enacts-groundbreaking-new-privacy-law>.
- [29] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. 2018. "If I press delete, it's gone" - User Understanding of Online Data Deletion and Expiration. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)* (2018).
- [30] Network Advertising Initiative. 2018. NAI Code of Conduct. (2018). https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.
- [31] Nielsen Norman Group. 2018. Top 10 Design Mistakes in the Unsubscribe Experience. (2018). <https://www.nngroup.com/articles/unsubscribe-mistakes/>.
- [32] Donald A. Norman. 1986. Cognitive Engineering. In *User Centered System Design: New Perspectives on Human-Computer Interaction*. Lawrence Erlbaum Associates, 31–61.
- [33] Donald A. Norman. 1990. *The Design of Everyday Things*. Doubleday.
- [34] Norwegian Consumer Council. 2018. Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy. (2018). <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.
- [35] Online Trust Alliance. 2018. Email Marketing & Unsubscribe Audit. (2018). <https://www.internetsociety.org/resources/ota/2018/2018-email-marketing-unsubscribe-audit/>.
- [36] Enric Pujol, Oliver Hohlfeld, and Anja Feldmann. 2015. Annoyed Users: Ads and Ad-Block Usage in the Wild. In *Proceedings of the Internet Measurement Conference*.
- [37] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*.
- [38] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. 2016. Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern. In *Proceedings of NDSS Workshop on Usable Security (USEC)*.
- [39] Fatemeh Shirazi and Melanie Volkamer. 2014. What Deters Jane from Preventing Identification and Tracking on the Web?. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*.
- [40] United States Congress. 1999. S.900 - Gramm-Leach-Bliley Act. (1999). <https://www.congress.gov/bill/106th-congress/senate-bill/00900>.
- [41] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.
- [42] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of Conference on Computer and Communications Security (CCS)*.
- [43] Ari Ezra Waldman. 2019. There is No Privacy Paradox: How Cognitive Biases and Design Dark Patterns Affect Online Disclosure. *Current Opinion in Psychology* (2019).

Shining a Light on Dark Patterns

Jamie Luguri* & Lior Jacob Strahilevitz**

Abstract

Dark patterns are user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. They typically exploit cognitive biases and prompt online consumers to purchase goods and services that they do not want, or to reveal personal information they would prefer not to disclose. Research by computer scientists suggests that dark patterns have proliferated in recent years, but there is no scholarship that examines dark patterns' effectiveness in bending consumers to their designers' will. This article provides the first public evidence of the power of dark patterns. It discusses the results of the authors' large-scale experiment in which a representative sample of American consumers were randomly assigned to a control group, a group that was exposed to mild dark patterns, or a group that was exposed to aggressive dark patterns. All groups were told they had been automatically enrolled in an identity theft protection plan, and the experimental manipulation varied what acts were necessary for consumers to decline the plan. Users in the mild dark pattern condition were more than twice as likely to remain enrolled as those assigned to the control group, and users in the aggressive dark pattern condition were almost four times as likely to remain enrolled in the program. There were two other striking findings. First, whereas aggressive dark patterns generated a powerful backlash among consumers, mild dark patterns did not – suggesting that firms employing them generate substantial profits. Second, less educated subjects were significantly more susceptible to mild dark patterns than their well-educated counterparts. Both findings suggest that there is a particularly powerful case for legal interventions to curtail the use of mild dark patterns.

The article concludes by examining legal frameworks for ameliorating the dark patterns problem. Many dark patterns appear to violate federal and state laws restricting the use of unfair and deceptive practices in trade. Moreover, in those instances where consumers enter into contracts after being exposed to dark patterns, their consent could be deemed voidable under contract law principles. The article proposes a quantitative bright-line rule for identifying impermissible dark patterns. Dark patterns are presumably proliferating because firms' secret and proprietary A-B testing has revealed them to be profit maximizing. We show how similar A-B testing can be used to identify those dark patterns that are so manipulative that they ought to be deemed unlawful.

* Law Clerk to the Honorable Brenda Sannes, United States District Court, Northern District of New York. J.D. University of Chicago Law School, 2019; Ph.D. Social Psychology, Yale University, 2015. The views expressed herein are solely those of the authors.

** Sidley Austin Professor of Law, University of Chicago. For helpful comments on earlier drafts and conversations the authors thank Omri Ben-Shahar, Sebastian Benthall, Adam Chilton, Brett Frischmann, Meirav Furth-Matkin, Todd Henderson, William Hubbard, Filippo Lancieri, Anup Malani, Florencia Marotta-Wurgler, Jonathan Masur, Jonathan Mayer, Richard McAdams, Terrell McSweeney, Paul Ohm, Roseanna Sommers, Geof Stone, Kathy Strandburg, Cass Sunstein, Blase Ur, Mark Verstraete, and Luigi Zingales, along with workshop participants at the University of Chicago's PALS Lab, the University of Chicago Works in Progress Workshop, and the Stigler Center's 2019 Antitrust and Competition Conference. The authors thank the Carl S. Lloyd Faculty Fund for research support and Tyler Downing and Daniel Jellins for excellent research assistance.

Table of Contents

Introduction.....	3
I. Dark Patterns in the Wild	6
II. An Experimental Test of the Effectiveness of Dark Patterns	17
A. Rates of Acceptance.....	21
B. The Influence of Stakes	23
C. Potential Repercussions of Deploying Dark Patterns	24
D. Predicting Dark Pattern Susceptibility.....	27
III. Are Dark Patterns Unlawful?.....	29
A. Laws Governing Deceptive and Unfair Practices in Trade	30
B. Other Relevant Federal Frameworks	37
C. Contracts and Consent	38
D. Line Drawing	43
E. Persuasion	46
Conclusion	48

Introduction

Everybody has seen them before and found them frustrating, but most consumers don't know what to call them. They are what computer scientists have (for the last decade) described as *dark patterns*,¹ and they are a proliferating species of sludge (to use a term preferred by behavioral economists)² or market manipulation (the moniker preferred by some legal scholars).³ Dark patterns are user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. They typically prompt users to rely on System 1 decision-making rather than more deliberate System 2 processes, exploiting cognitive biases like framing effects, the sunk cost fallacy, and anchoring. The goal of most dark patterns is to manipulate the consumer into doing something that is inconsistent with her preferences, in contrast to marketing efforts that are designed to alter those preferences. The first wave of academic research into dark patterns identified the phenomenon and developed a typology of dark pattern techniques.⁴

This summer, computer scientists at Princeton and the University of Chicago took a second step towards tackling the problem by releasing the first major academic study of the prevalence of dark patterns.⁵ Arunesh Mathur and six co-authors developed a semi-automated method for crawling more than 11,000 popular shopping websites. Their analysis revealed the presence of dark patterns on more than 11% of those sites, and the most popular sites were also most likely to employ dark patterns.⁶

If the first wave of scholarship created a useful taxonomy and the second step in the scholarship established the growing prevalence of dark pattern techniques then it seems clear where the literature ought to go next. Scholars need to quantify the effectiveness of dark patterns in convincing online consumers to do things that they would otherwise prefer not to

¹ User interface designer Harry Brignull coined the phrase in 2009 and maintains a web site that documents them in an effort to shame the programmers behind them. See <https://www.darkpatterns.org/>

² Cass R. Sunstein, *Sludges and Ordeals*, 69 DUKE L.J. ____ (forthcoming 2019); Richard H. Thaler, *Nudge, Not Sludge*, 361 SCIENCE 431 (2018). A sludge is an evil "nudge," one that exploits their cognitive biases to persuade them to do something that is undesirable, typically by introducing excessive friction into choice architecture. See Cass R. Sunstein, *Sludge Audits*, Harvard Public Law Working Paper No. 19-21 (July 2, 2019 draft), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379367 (hereinafter Sunstein, *Sludge Audits*).

³ Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 NYU L. REV. 632 (1999).

⁴ See, e.g., Christoph Bösch et al., *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, *Proceedings on Privacy Enhancing Technologies* (2016); Colin M Gray et al., *The Dark (Patterns) Side of UX Design*, *PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS* (2018).

⁵ Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, July 17, 2019 working paper, available at <https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf>.

⁶ As the authors themselves note, see *id.* at 2, this figure probably understates the prevalence of dark patterns, because their taxonomy of dark patterns leaves out several important dark pattern mechanisms, perhaps in part because they are hard to identify using the semi-automated approach employed by the authors. See *infra* table 1 (providing a taxonomy that omits nagging, bait and switch, aesthetic manipulation and other important types of dark patterns).

do. In short, the question we pose in this paper is “how effective are dark patterns?” That is not a question that has been answered in academic research to date. But it is a vital inquiry if we are to understand the magnitude of the problem and whether regulation is appropriate.

To be sure, the lack of published research does not mean that the effectiveness of these techniques is a complete mystery. On the contrary, we suspect that the kind of research results we report here have been replicated by social scientists working in-house for technology and ecommerce companies. Our hunch is that consumers are seeing so many dark patterns in the wild because the internal, proprietary research suggests dark patterns are presently profit-maximizing for the firms that employ them. But those social scientists have had strong incentives to suppress the results of their A-B testing of dark patterns, so as to preserve data about the successes and failures of the techniques as trade secrets and (perhaps) to stem the emergence of public outrage and legislative or regulatory responses.

With bipartisan legislation that would constrain the use of dark patterns currently pending in the Senate,⁷ investigative reporters beginning to examine the dark patterns problem,⁸ and one of the nation’s leading privacy scholars testifying before the Federal Trade Commission (F.T.C.) that in his estimation, 2019 would be the year of the dark pattern,⁹ e-commerce firms probably expect that, where the effectiveness of dark patterns is concerned, heat will follow light. So they have elected to keep the world in the dark for as long as possible. The strategy has worked so far.

The basic problem of manipulation in marketing and sales is not unique to interactions between computers and machines. The main factors that make this context interesting are its relative newness and scale. In both traditional and online contexts legal actors have to make tough decisions about where the precise line is between persuasion and manipulation, and what conduct is misleading enough to eliminate what might otherwise be constitutionally protected rights for sellers to engage in commercial speech. The law has long elected to prohibit certain strategies for convincing people to part with money or personal information. Laws prohibiting fraud have been around, seemingly forever, and more recently implemented laws proscribe pretexting. States and the federal government have given consumers special rights in settings characterized by high pressure, mild coercion, or vulnerability, such as door-to-door-sales, and transactions involving funeral services, timeshares, telemarketing, or home equity loans. Sometimes the law enacts outright prohibitions with substantial penalties. Other times it creates cooling off periods that cannot be waived. A key question we address is what online tactics are egregious enough to warrant this kind of special skepticism.

⁷ Deceptive Experiences to Online Users Reduction Act (DETOUR Act), Senate Bill 1084, 116th Congress, introduced April 9, 2019, text available at <https://www.congress.gov/bill/116th-congress/senate-bill/1084/text>.

⁸ See, e.g., Jennifer Valentino-Devries, *How E-Commerce Sites Manipulate You into Buying Things You May Not Want*, N.Y. TIMES, June 24, 2019, at B1.

⁹ See F.T.C. Hearing, Competition and Consumer Protection in the Twenty-First Century, April 9, 2019, Testimony of Professor Paul Ohm, Georgetown University, Transcript at 49 (“my prediction for 2019 ... is this is the year where dark patterns really becomes the kind of thing that we’re really talking a lot about.”), available at https://www.FTC.gov/system/files/documents/public_events/1418273/FTC_hearings_session_12_transcript_day_1_4-9-19.pdf.

Ours is a descriptive paper, an empirical paper, a normative paper, and then a descriptive paper again. That said, the new experimental data we reveal is the most important take-away. Part I begins by describing dark patterns – what techniques they include and what some of the most prominent examples are. The description illuminates several real-world dark patterns and suites of dark patterns employed by major multinational corporations. The Part also provides a streamlined taxonomy of dark pattern techniques, one that builds on work that computer scientists have done while providing some conceptual clarity that’s caused scholars of human-computer interactions to lump together divergent phenomena.

Part II provides the paper’s core contribution. As scholars have seen the proliferation of dark patterns, many have assumed that dark patterns are efficacious. Why else would large, well-capitalized companies that are known to engage in A-B testing be rolling them out? Judges confronting dark patterns have for the most part shared these intuitions, though not universally. We show that many widely employed dark patterns prompt consumers to do what they would not do in a more neutral decision-making environment. But beyond that, we provide the first comparative evidence that quantifies how well they work, and that sheds some light on the question of which techniques work best. Our bottom line is that *dark patterns are strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces*. Relatively mild dark patterns more than doubled the percentage of consumers who signed up for a dubious identity theft protection service that we told our subjects we were selling, and aggressive dark pattern nearly quadrupled the percentage of consumers signing up. In social science terms, the magnitudes of these effects are enormous. We then provide powerful evidence that dosage matters – aggressive dark patterns generate a powerful customer backlash. Mild dark patterns usually do not, and therefore, counterintuitively, the strongest case for regulation and other legal intervention concerns subtle uses of dark patterns. Finally, we provide compelling evidence that less educated Americans are significantly more vulnerable to dark patterns than their more educated counterparts, and that trend is particularly pronounced where subtler dark patterns are concerned. This observation raises distributive issues and is also useful as we consider how the law might respond to dark patterns.

Part III looks at the existing law and asks whether it prohibits dark patterns. This is an important area for inquiry because pending bipartisan legislation proposes that the F.T.C. be given new authority to prohibit dark patterns.¹⁰ It turns out that with respect to a number of central dark pattern techniques, the F.T.C. is already going after some kinds of dark patterns, and the federal courts have been happy to cheer the agency along. The most successful actions have nearly all fallen under the F.T.C.’s section five authority to regulate deceptive acts and practices in trade. To be sure, other important dark patterns fit less comfortably within the categories of deceptive or misleading trade practices, and there is lingering uncertainty as to how much the F.T.C.’s authority to restrict unfair trade practices will empower the agency to restrict that behavior. The passage of federal legislation aimed squarely at dark patterns would provide useful new legal tools, but there is no reason to delay enforcement efforts directed at egregious dark patterns while waiting on Congress to do something.

Of course, the F.T.C. lacks the resources to be everywhere, so a critical issue going forward will be whether contracts that are agreed to in large measure because of a seller’s use of dark patterns are deemed valid. This issue is just now starting to bubble up in the case law. To deal with this question, and other important line-drawing questions, we propose a quantitative

¹⁰ See *supra* text accompanying note 7.

“more likely than not” approach to regulation. The method we use in this paper is easy to replicate, and the math is not especially fancy. Where the use of a dark pattern technique more than doubles the rate of acceptance compared to neutral choice architecture, the law should regard the dark pattern’s use as per se unlawful. To be sure, that is an underinclusive test, one that should be supplemented by a balancing inquiry. But we think it is a good and straightforward place to start as the law begins to grapple seriously with the question of how to regulate dark patterns. Notably, both the mild and aggressive dark patterns we tested experimentally satisfied that test. As we explain in Part III, there is a plausible case to be made that agreements procured through the use of dark patterns are voidable as a matter of contract law under the undue influence doctrine.

We said at the outset that dark patterns are different than other forms of dodgy business practices because of the scale of e-commerce. There may be poetic justice in the notion that this very scale presents an opportunity for creative legal regulators. It is exceedingly difficult to figure out whether a door to door salesperson’s least savory tactics significantly affected the chances of a purchase – was the verbal sleight of hand material or incidental? Who knows? But with e-commerce, firms can run thousands of consumers through identical interfaces at a reasonable cost and see how small tweaks to the software might alter user behavior. Social scientists working in academia or for the government can do this too; we just haven’t done so before today. Now that scholars can test dark patterns, we can isolate causation in a way that’s heretofore been impossible in the brick-and-mortar world. Unlike brick-and-mortar manipulation, dark patterns are hiding in plain sight, operate on a massive scale, and are relatively easy to detect. Those facts strengthen the case further for the legal system to address their proliferation.

So let’s spend some time getting to know dark patterns.

I. Dark Patterns in the Wild

Suppose you are getting commercial emails from a company and wish to unsubscribe. If the company is following the law they will include in their emails a link to a page that allows you to remove your email address.¹¹ Some companies make that process simple, automatically removing your address when you click on an unsubscribe link or taking you to a page that asks you to type in your email address to unsubscribe. Once you do so they will stop sending you emails.

Other companies will employ various tools to try to keep you on their lists. They may remind you that if you unsubscribe you will lose out on valuable opportunities to save money on their latest products (dark patterns researchers call this practice “confirmshaming”). Or they’ll give you a number of options besides the full unsubscribe that most people presumably want, such as “receive emails from us once a week” or “receive fewer emails from us” while making users who want to receive no more emails click through to a subsequent page.¹² (These

¹¹ This is required by the CAN-SPAM Act of 2003, 15 U.S.C. § 103.

¹² As of July 2019, Best Buy’s unsubscribe link in commercial emails followed this pattern. If a user clicked on the unsubscribe hyperlink at the bottom of a marketing email, she would be taken to a screen that provided three options: “Receive all General Marketing emails from Best Buy.” [This box is checked by default, so a user who clicks “unsubscribe” and then “submit” will not stop receiving emails from Best Buy.] The second option says, “Receive no more than one General Marketing email per week.” And the third option is “Receive no General Marketing emails (unsubscribe).”

techniques are referred to as “obstruction” dark patterns).¹³ The company is making it easy for you to do what it prefers (you continue to receive lots of marketing emails), and harder for you to do the thing it can live with (receiving fewer emails), or the thing you probably prefer and are entitled to by law (receiving no emails from the company).

In other instances, firms employ highly confusing “trick question” prompts that make it hard for even smart consumers to figure out how they are to accomplish their desired objective. For instance, see the membership cancellation page from the Pressed Juicery:¹⁴

Membership Status

Canceling your membership?

Are you sure you want to cancel your membership? You will no longer receive membership pricing on all our products.

CONTINUE

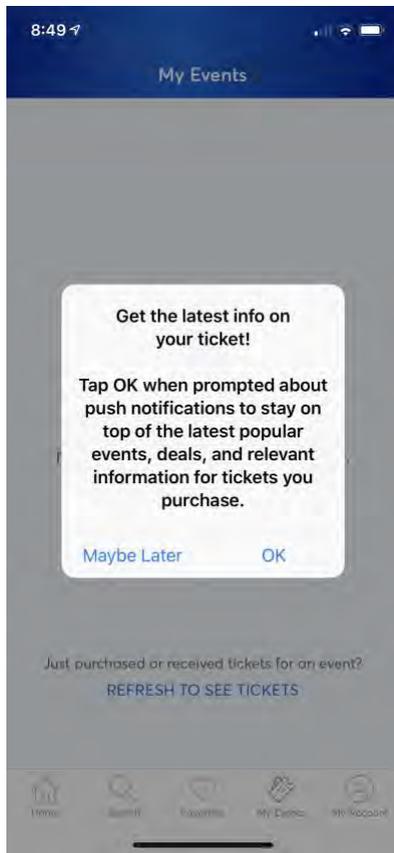
CANCEL

Other aggravating examples of dark patterns abound. If you have found it easy to sign up for a service online, with just a click or two, but when it came time to cancel the service had to make a phone call or send a letter via snail mail, you have been caught in a “roach motel” dark pattern (it’s easy to get in but hard to get out). If you’ve ever seen an item in your shopping cart that you did not add to it and wondered how it got there, you have encountered a “sneak into the cart” dark pattern. If you’ve once been given a choice between signing up for notifications, with the only options presented being “Yes” and “Not Now,” only to be asked again about signing up for notifications two weeks later when you select “Not Now,” that’s a “nagging” dark pattern. Here is one from Ticketmaster’s smartphone app.¹⁵

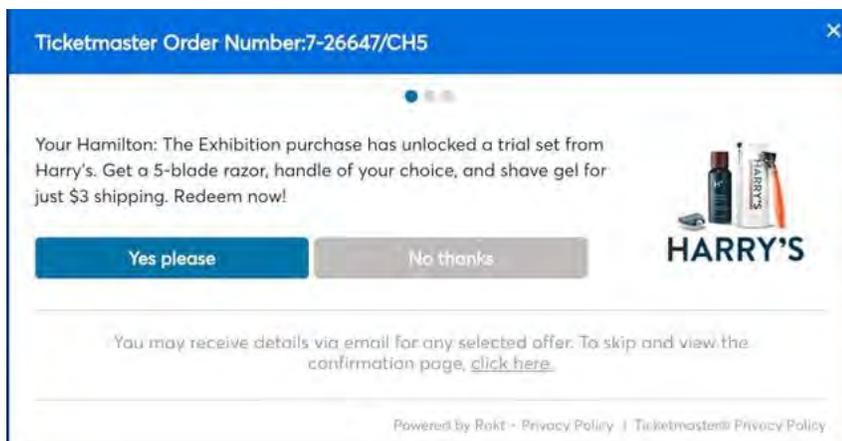
¹³ Gray et al., *supra* note 4, at 5-6; LIOR STRAHILEVITZ ET AL., SUBCOMMITTEE REPORT: PRIVACY AND DATA PROTECTION, STIGLER CENTER COMMITTEE FOR THE STUDY OF DIGITAL PLATFORMS 22-23 (2019).

¹⁴ For this example, we thank Karin Curkowicz. See <https://twitter.com/KCurkowicz/status/1137855721507213312>

¹⁵ Google Maps does essentially the same thing. When a user repeatedly travels to a particular location and uses the app’s directions, the app will display a “Go here often?” pop-up window that asks whether the location is her “Home,” “Work,” or “Other” (school, gym, etc.) approximately once a week. A user can close the window each time but there is evidently no way to prevent the queries from reappearing short of deleting all location history. The pop-up window notes that users’ labels for locations “will be used across Google products, for personalized recommendations, and for more useful ads.”



Bait and switch is another time-tested dodgy business practice, and the tactic has emerged online as a type of dark pattern. Sometimes it arises in its classic form, and sometimes it emerges as a bait-and-sell and switch, where the customer does get to purchase the good or service that was advertised, but is then shown a barrage of ads for things the customer does not want. Here is an example of the latter from one of the author's recent online purchases from the aforementioned Ticketmaster.



Alexander Hamilton was generally depicted clean-shaven in portraits.¹⁶ Other than that, it's not clear what the connection is between the ticket purchase and a razor-blade subscription. Notice further that besides bait and switch there are two subtler dark patterns embedded in the image above. In the ad, "Yes please" appears against a bright blue background while "No thanks" appears less legible against a gray one. Moreover, another even lighter gray font (barely legible in the pop-up ad) reveals important text about what a consumer has to click on to skip the several bait-and-switch ads that would follow, which in this case included further offers from Hotels.com, Priceline, and Hulu. The font appears much less prominently than the darker text above it about the razor blade offer.

Another common dark pattern is generating false or misleading messages about demand for products or testimonials. Arunesh Mathur and co-authors recently revealed that a number of popular shopping sites display information about recent sales activities that is driven by random number generators and similar techniques. For example, they caught thredup.com using a random number generator to display information about how many of a particular product were "just sold" in the last hour, and they found various sports jersey sales sites using identically phrased customer testimonials but with different customer names each time.¹⁷ When a site notes that Anna in Anchorage just purchased a jacket that a user is examining, the academic research suggests these high-demand messages should be taken with a large grain of salt.

Having introduced a few vivid examples of dark patterns, it seems appropriate to introduce a workable taxonomy of the techniques. Several have been developed in the existing literature. One problem is that as interest in dark patterns has grown, so has the ostensible list of what counts as one. Putting together the various taxonomies in the literature results in a rather lengthy list, with some techniques being very problematic and others less so. There have been four key taxonomies to emerge in the dark patterns literature, with each building on and tweaking what came before. The chart below reproduces the current aggregated taxonomy in the literature and identifies which types of dark patterns have been identified in multiple taxonomies versus only some.¹⁸ Our literature review reveals eight categories of dark patterns and 27 variants.¹⁹ After presenting this information we will propose a modified, streamlined taxonomy that appropriately focuses on the means (the manipulative techniques used) rather than the ends (getting users to provide sensitive information, cash, recruit others, etc.). It is worth noting at the outset that some of the choices different teams of scholars have made in presenting their taxonomies relate to their different objectives. For example, some scholars, like Bösch et al, are not trying to be comprehensive. Others, like Mathur et al., are focusing on the sorts of dark patterns that can be identified using a semi-automated web-crawling process. Such processes lend themselves to flagging certain kinds of dark patterns (such as low-stock messages) more readily than others (such as toying with emotions).

¹⁶ Alas, so was Aaron Burr.

¹⁷ Mathur et al., *supra* note 5, at 18-19.

¹⁸ Most of the dark patterns literature is co-authored. For space-saving reasons, we include in the table only the surname of the first listed author of such work.

¹⁹ We apologize for the small font size necessary to squeeze the table onto a page. We promise the table is not intended to be a dark pattern – we actually want you to read the categories and examples closely.

Table 1: Summary of Existing Dark Pattern Taxonomies

Category	Variant	Description	Source
Nagging		Repeated requests to do something firm prefers	Gray
Social Proof	Activity messages	False / misleading Notice that others are purchasing, contributing	Mathur
	Testimonials	False / misleading positive statements from customers	Mathur
Obstruction	Roach Motel	Asymmetry between signing up and canceling	Gray, Mathur
	Price Comparison Prevention	Frustrates comparison shopping	Brignull, Gray, Mathur
	Intermediate Currency	Purchases in virtual currency to obscure cost	Brignull
	Immortal Accounts	Account and consumer info cannot be deleted	Bösch
Sneaking	Sneak into Basket	Item consumer did not add is in cart	Brignull, Gray, Mathur
	Hidden Costs	Costs obscured / disclosed late in transaction	Brignull, Gray, Mathur
	Hidden subscription / forced continuity	Unanticipated / undesired automatic renewal	Brignull, Gray, Mathur
	Bait & Switch	Customer sold something other than what's originally advertised	Gray
Interface Interference	Hidden information / aesthetic manipulation	Important information visually obscured	Gray
	Preselection	Firm-friendly default is preselected	Bösch, Gray
	Toying with emotion	Emotionally manipulative framing	Gray
	False hierarchy / pressured selling	Manipulation to select more expensive version	Gray, Mathur
	Trick questions	Intentional or obvious ambiguity	Gray, Mathur
	Disguised Ad	Consumer induced to click on something that isn't apparent ad	Brignull, Gray
	Confirmshaming	Choice framed in way that makes it seem dishonorable, stupid	Brignull, Mathur
	Cuteness	Consumers likely to trust attractive robot	Lacey
Forced Action	Friend spam / social pyramid / address book leeching	Manipulative extraction of information about other users	Brignull, Bösch, Gray
	Privacy Zuckering	Consumers tricked into sharing personal info	Brignull, Bösch, Gray
	Gamification	Features earned through repeated use	Gray
	Forced Registration	Consumer tricked into thinking registration necessary	Bösch
Scarcity	Low stock message	Consumer informed of limited quantities	Mathur
	High demand message	Consumer informed others are buying remaining stock	Mathur
Urgency	Countdown timer	Opportunity ends soon with blatant visual cue	Mathur
	Limited time message	Opportunity ends soon	Mathur

Now let's see if we can do a little bit of streamlining. In our view, dark patterns are techniques used to manipulate users to do things they would not otherwise do. Precisely what users wind up doing is irrelevant for our purposes, so long as it is something they do not genuinely want to do. This warrants removal of dark pattern techniques included above that are focused on ends rather than means.

Immortal accounts are a privacy-focused ostensible dark pattern, one that obstructs the deletion of information the customer may want to make disappear. Because the technique focuses on ends (privacy protection) rather than the mechanism used, we don't include it as a dark pattern. The same can be said about friend spam and privacy zuckering. Making robots cute to get people to share intimate details about themselves (which Lacey and Caudwell have dubbed a dark pattern)²⁰ is not appropriately characterized in that way. Part of the reason why is the ends-orientation identified above.²¹ Gamification and non-misleading forms of forced registration are not dark patterns for different reasons. In our view, if a company wants to structure the quid pro quo that's central to their business model as "you give us personal information in exchange for stuff," this is permissible. So an online newspaper can decide to provide content for free in exchange for the user accurately identifying himself to facilitate subsequent marketing. As long as the nature of the exchange isn't concealed, it's not a dark pattern. So too with a business model that privileges highly engaged users over occasional ones. Finally, it seems to us that in the Mathur et al. framework "Scarcity" and "Urgency" are exploiting the same behavioral mechanisms to induce a type 1 purchase or disclosure decision. They can be collapsed for analytical purposes into a single category. Our edits produce the following revised taxonomy that is a bit easier on the eyes (and perhaps the brain).

²⁰ Cherie Lacey & Catherine Caudwell, *Cuteness as a 'Dark Pattern' in Home Robots*, in 14TH ACM/IEEE INT'L CONF. ON HUMAN-ROBOT INTERACTION (HRI) CONFERENCE PROCEEDINGS 374 (2019), available at <https://ieeexplore.ieee.org/abstract/document/8673274>.

²¹ A deeper concern related to stretching the dark pattern label that far is the problem of identifying what a neutral baseline looks like. As we will argue below, if a neutral interface can be identified and then compared to an ostensibly manipulative one, we can use quantitative techniques to resolve lingering uncertainty about when a sales technique crosses the line. But it's hard to say what a "neutrally cute" robot looks like. More broadly, it has long been true that sellers of goods use conventionally attractive people to sell not only obvious products like fashion and jewelry but also less obvious products like detergent and insurance. The "cute robot" strategy is a variant of that. While it is possible to use A-B testing to identify the precise impact that a conventionally attractive model versus an average-looking model has on the sales of toothpaste, the lack of deception used in such advertisements and the extremely long pedigree of such techniques in advertising make this a poor fit for the category. Further, our prior is that the effect sizes from those techniques would be nontrivial but not especially large.

Table 2: Revised Taxonomy of Dark Patterns

Category	Variant	Description	Source
Nagging		Repeated requests to do something firm prefers	Gray
Social Proof	Activity messages	Misleading notice about other consumers' actions	Mathur
	Testimonials	Misleading statements from customers	Mathur
Obstruction	Roach Motel	Asymmetry between signing up and canceling	Gray, Mathur
	Price Comparison Prevention	Frustrates comparison shopping	Brignull, Gray, Mathur
	Intermediate Currency	Purchases in virtual currency to obscure cost	Brignull
Sneaking	Sneak into Basket	Item consumer did not add is in cart	Brignull, Gray, Mathur
	Hidden Costs	Costs obscured / disclosed late in transaction	Brignull, Gray, Mathur
	Hidden subscription / forced continuity	Unanticipated / undesired automatic renewal	Brignull, Gray, Mathur
	Bait & Switch	Customer sold something other than what's originally advertised	Gray
Interface Interference	Hidden information / aesthetic manipulation / false hierarchy	Important information visually obscured	Gray, Mathur
	Preselection	Firm-friendly default is preselected	Bösch, Gray
	Toying with emotion	Emotionally manipulative framing	Gray
	Trick questions	Intentional or obvious ambiguity	Gray, Mathur
	Disguised Ad	Consumer induced to click on something that isn't apparent ad	Brignull, Gray
	Confirmshaming	Choice framed in way that seems dishonest / stupid	Brignull, Mathur
Forced Action	Forced Registration	Consumer tricked into thinking registration necessary	Bösch
Urgency	Low stock / high-demand message	Consumer falsely informed of limited quantities	Mathur
	Countdown timer / Limited time message	Opportunity ends soon with blatant false visual cue	Mathur

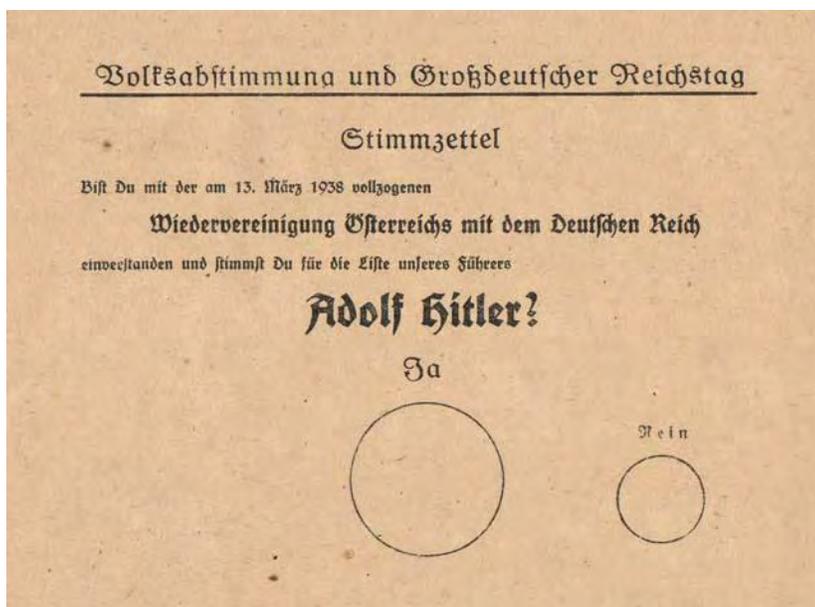
That revised taxonomy of dark patterns is still lengthy, but it's hopefully easier to internalize. As we will see, in many instances firms are going to combine several of the techniques on this list. We previously singled out Ticketmaster, a major American company with a large market share. So we'll end our introduction to dark patterns with an extended exploration of techniques employed by Sony, a major Japanese company with a large market share.

As gaming platforms have become a major source of revenue, the dominant platforms have sought to profit off the increased appeal of online gaming. Online gaming allows individuals to play over the Internet against friends or strangers, and both Sony and Microsoft have made major investments in this technology. One strategy that is widely employed in popular games makes it necessary for players to sign up for the online platforms in order to earn the most appealing available rewards. One of the authors has a child who enjoys EA's FIFA soccer games on the Sony PlayStation, and to that end, the author signed up for a short-term subscription to PlayStation Plus – Sony's online gaming platform. During the next few paragraphs we will use Sony's user interface as a case study of dark patterns.

Let's begin with Sony's pricing model and graphic design choices.



Several notable aspects of the user interface stand out. First, notice the visual prominence of the 12 month subscription rather than the alternatives in the default view. This “false hierarchy” graphic design approach is a kind of dark pattern; one with a long and infamous history, at that.



Translation: “Do you agree with the reunification of Austria with the German Reich that was enacted on 13 March 1938 and do you vote for the party of our leader; Adolf Hitler?; Yes (large circle); No (small circle)”

Choice-architects have long understood that contrasting visual prominence can be used to nudge choosers effectively into a choice the architect prefers, and false hierarchy can come in handy whether one is an innovative multinational technology company or a group of genocidal fanatics conducting a sham election.²² The visual contrast is one of the least subtle and presumably more benign dark patterns that can be encountered in the wild. Unlike many dark patterns identified above, it is almost certainly a legal marketing tactic when used in isolation.²³

²² It hopefully goes without saying that our juxtaposition is not equating the Sony Corporation with Nazi Germany.

²³ Most of the brick-and-mortar equivalent of dark pattern techniques on our list are either very uncommon or are widely believed to be dubious or unlawful when practiced in brick and mortar establishments. For example, telemarketers are prohibited from engaging in various forms of nagging, such as continuing to call someone who has said she does not wish to receive such calls. 10 C.F.R. 310.4(b)(1)(iii)(A). To take another example, the F.T.C. has issued a policy statement making it clear that the use of disguised ads is actionable under section 5. See F.T.C., Enforcement Policy Statement on Deceptively Formatted Advertisements (Dec. 22, 2015), available at https://www.FTC.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf. And some brick and mortar equivalents of dark patterns are so obviously unlawful that reputable firms do not even try them. For example, suppose Trader Joe’s instructed its cashiers to start charging their customers for granola bars they did not purchase and slipping those bars into their shopping carts surreptitiously. Surely some customers who didn’t notice what happened in the check-out aisle will not wind up returning the granola bars because of the inconvenience involved, but that hardly means there is no injury from the conduct, nor would we be comfortable describing the transaction as one in which the customers consented to purchase the granola bars. The online equivalent of that conduct is “sneak into basket.” It’s hard to imagine what a coherent defense of the tactic at a grocery store would look like.

Now let's consider Sony's pricing strategy. It is no mystery what Sony is trying to do. They want to minimize customer churn. Acquiring subscribers is quite costly, so Sony wants to retain them once they obtain them. Moreover, some customers may subscribe for a year because of the lower per-month rate (\$5 per month versus \$10 per month), and then grow bored with the service – these customers are good for Sony because they will be paying for network resources that they do not use, which will improve the experience for other paying customers. It's akin to people joining a gym as a New Year's resolution and then never showing up after January to use the treadmills. One way to get customers to commit to a longer term is by substantially discounting the monthly cost for customers who are willing to sign up for a year's membership. In this instance, Sony is willing to charge such customers half as much as customers who will only commit to subscribing for a month. To be clear, there is nothing legally wrong with Sony pursuing this pricing model and (at least from our perspective) there is not anything morally dubious about the practice either, at least not yet. The pricing model is not a dark pattern.

It's on the following screen that things get dicey. Suppose someone opts to pay a higher monthly fee and sign up for a one-month subscription. This user is presumably unsure about how much she will enjoy PlayStation Plus, so she is paying double the lowest monthly fee in exchange for the right to cancel her subscription if she doesn't enjoy the service all that much. If the customer selects that option, she will soon see this screen:



Ok. So customers who sign up for a one-month membership at \$10 per month will have that membership automatically renewed, at twice the monthly cost of customers who sign up for a 12-month membership. Presumably a tiny fraction of one-month subscribers prefer autorenewal at a high monthly rate. But never fear, as the figure above shows, Sony will let those customers opt out of automatic renewal, provided they click through . . . at least five screens – Settings, Account Managements, Account Information, Wallet, and Purchase Settings, where they will see a button that lets them toggle off autorenewal.²⁴ A user who neither writes down the precise opt-out instructions nor takes a digital photograph of the screen above will be lost at sea – the different steps a user must go through are far from intuitive.

²⁴ It's actually even more cumbersome. When one of the authors opted to turn off automatic renewal the author was required to re-log in to the system with a username and password, even though the author was already logged in.

A cynical observer might view Sony as furthering two objectives here. First, Sony knows that a number of their one-month subscribers will be auto-renewed at a high monthly rate, and that's a lucrative source of revenue for the company. Second, Sony knows that some of its customers will grasp immediately how difficult opting out of automatic renewal is, think it through a bit, and then press cancel. Presumably most will then sign up for the twelve-month subscription that Sony probably prefers, whose automatic renewal feature is less blatantly problematic. Either way, Sony comes out ahead.

When evaluating potential dark patterns, we need to be sure that we can differentiate between true positives and false positives. So in this instance we would want to know whether Sony's user interface is the product of an intentional design choice, an accident, or an external constraint. We will admit to a lack of hard data on this (in contrast to the remainder of this data-heavy paper) but in retrospect it seems clear that almost nobody who signs up for a one-month subscription at a high rate will also prefer for that subscription to autorenew. Where we see a user interface nudge consumers towards a selection that is likely to be unpopular with them but profitable for the company, there is reason to think a dark pattern may exist.²⁵ But perhaps Sony's programmers didn't think of that at the time. Alternatively, maybe letting people opt out of autorenewal for a PlayStation Plus subscription on one screen is inherently cumbersome for one reason or another. In this instance, we can more or less rule out the innocent explanations. Tellingly, once a customer signs up for autorenewal Sony will let them turn it off without navigating through five or more screens.



The initial set-up and very difficult process for opting out of autorenewal at the outset seems to be a conscious and intentional choice by Sony. If we examine what Sony is doing through the lens of existing taxonomies we can see that it is combining several tactics that have been identified as dark patterns.

²⁵ The connection between the majority sentiment among consumers and the identification of dark patterns is explored more explicitly in STRAHILEVITZ ET AL., *supra* note 13, at 44. In this paper's companion piece, we devote more time and experimental energy towards identifying the expectations and preferences that most consumers share. See Lior Jacob Strahilevitz & Jamie Luguri, *Consumertarian Default Rules*, __ J. CONTEMP. PROBLEMS __ (forthcoming 2020); see also Franklin G. Snyder & Ann M. Mirabito, *Consumer Preferences for Performance Defaults*, 6 MICH. BUS. & ENTREPRENEURIAL L. REV. 35 (2016) (reporting the results of survey research into consumer preferences in other sales contexts).

In this instance, Sony is combining a false hierarchy (the different sizes of the buttons on the initial screen), the bait and switch (the one-month subscription looks like it offers an easy way to decline the product after the user experiences it, but given user inertia it's often an indefinite subscription with a higher monthly rate), preselection (the default choice is good for the company and bad for most one-month subscription consumers), a roach motel (opting out of automatic renewal is far more difficult and time-consuming than keeping the automatic renewal); and forced continuity (many users will wind up paying for the service for a lengthy period of time despite their initial intent not to do so). These dark patterns are used in combination, seemingly in an effort to manipulate users into either a long-term subscription or an automatically renewing indefinite subscription at a high monthly rate.

To review, there are a variety of dark patterns that are designed to nudge consumers into contractual arrangements that they presumably would not otherwise prefer, and these techniques appear to be employed by a variety of different ecommerce firms, from start-up apps to well-capitalized platforms like Ticketmaster and Sony. Ticketmaster and Sony have a lot of smart people who work for them, so one assumes that they are doing what they are doing because it is good for the firms' bottom lines. But beyond that intuition we lack reliable information about the effectiveness of these dark patterns in nudging consumers to behave in ways that maximize firm profits. Turning to Part II of our paper, which is the heart of the project, we will now attempt to fill that gap in the literature. In order to do that, we created a classic "bait and switch" scenario with a large sample of Americans online.

II. An Experimental Test of the Effectiveness of Dark Patterns

Let's suppose Amazon or Microsoft was interested in testing the effectiveness of dark patterns. It would be easy to do so using their existing platform. They have an ongoing relationship with millions of customers, and many of them have already stored their credit card information to enable one-click purchasing. So they could beta-test different dark patterns on subsets of their user-base, exploiting randomization, and then track purchases and revenue to see what works. The risks of customer / employee blowback or legal liability would be the main constraints on what they could do.

For academics seeking to test the efficacy of dark patterns, the challenge is much more significant. Academic researchers generally do not have established relationships with customers (students aside, and that relationship is heavily regulated where financial aid and tuition payment are concerned). The point of a dark pattern typically is to manipulate people to pay for something they otherwise would not purchase or surrender personal information they would otherwise keep confidential. There has been a little bit of academic work that has studied how different user interfaces can encourage the latter,²⁶ and none on the former. Because we are most interested in understanding how effective dark patterns are at parting consumers with their money, we wanted to situate ourselves in Amazon or Microsoft's shoes to the fullest extent possible. Alas, setting up a new ecommerce platform to run those experiments was prohibitively expensive.

²⁶ See, e.g., Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOCIAL PSYCH. & PERSONALITY SCIENCE 340 (2012); Leslie K. John et al., *Strangers on a Plane: Context-Dependent Willingness to Disclose Sensitive Information*, 37 J. CONSUMER RES. 858 (2011); Marianne Junger et al., *Priming and Warnings Are Not Effective to Prevent Social Engineering Attacks*, 66 COMPUTERS IN HUM. BEHAV. 75 (2017).

To that end, we designed a bait-and-switch scenario that would strike consumers as plausible. We would use an existing survey research firm to recruit a large population of American adults to participate in a research study that would evaluate their attitudes about privacy. Then we would deceive those adults into believing, at the end of the survey, that because they expressed a strong interest in privacy (as respondents typically do in surveys) we had signed them up for a costly identity-theft protection service and would give them the opportunity to opt out. We would structure the experiment in a way so as to make experimental subjects believe that their own money was at stake and they would incur a legal obligation to pay for the service if they did not opt out, even though we did not have their credit card or bank payment information. Then we would randomly vary whether the opportunity to opt out was unconstrained or impeded by different dosages of dark patterns. This manipulation would plausibly generate information about consumers' revealed preferences, and it would allow us to do so without actually selling any goods or services to consumers. Our host university's I.R.B. approved our proposal to engage in the deceptive experiment after we explained, among other things, (a) that we wouldn't actually store any of the information that we were purportedly collecting to uniquely identify our experimental subjects, and (b) that we would promptly debrief participants at the end of the survey so they understood they would not be charged any money for our non-existent identity theft protection service.

To put that research plan in motion, we administered an online survey to a nationally representative (census weighted) sample of American participants recruited by Dynata, a professional survey research firm. We removed respondents who took too long or too little time to complete the survey from the sample, as well as those who failed an attention check.²⁷ This left a final sample of 1,963 participants.²⁸ Participants were compensated by Dynata for their time, and we compensated Dynata. We pre-registered the experiment with AsPredicted.Org.²⁹

To begin, study participants answered various demographic questions including age, gender, race, education, income, employment, political orientation, and region of the country. Included with these basic demographic questions were additional questions aimed to bolster

²⁷ After removing two participants who started and ended the survey on different days, the average completion time was computed. Participants took 11.5 minutes on average to complete the survey. We removed participants who took less than 4 minutes and more than 47.5 minutes (two standard deviations above the survey completion time). Additionally, participants were asked an attention check question that asked them to "Please select "Strongly agree" for this question below to show that you are paying attention." Those that failed to answer accordingly were removed from the sample. At the end of the survey participants were asked to indicate how seriously they took the survey on a scale from 1 ("not at all seriously") to 5 ("extremely seriously"). Participants who answered 1 were also removed from the sample.

²⁸ Males comprised 47.1% of the sample. 76.2% of the sample self-identified as White, 13.2% as Black, 1.2% as American Indian, 4.4% as Asian, and 4.9% as "other." On a separate question, 14% indicated they are Hispanic or Latino. 6% of the sample had not completed high school, 29.8% had high school diplomas, 29.8% had some college or an associate's degree, 20.9% had bachelor's degrees, and 13.6% had advanced degrees. 10.8% of the sample was between 18-24 years old, 18% was between 25-34, 17.6% was between 35-44, 17.2% was between 45-54, 19.3% was between 55-64, and 17% was 65 years or older. 1773 participants (90.3%) fully completed the survey from start to finish.

²⁹ See https://aspredicted.org/see_one.php (Experiment # 19680) (submitted Feb. 17, 2019). On the value of pre-registration in social science research, see Brian A. Dosek et al., *The Preregistration Revolution*, 115 PNAS 2600 (2018).

the later cover story that we had pinpointed their mailing address. Specifically, participants were asked their zip code, how long they had lived at their current residence, their telephone number, and where they were completing the survey (home, work, or other).³⁰

Participants then filled out the Ten Item Personality Measure, an instrument designed to measure the Big Five personality dimensions (extraversion, agreeableness, conscientiousness, emotional stability, and openness to experiences).³¹ We included this measure to test whether certain personality traits would predict susceptibility to dark pattern manipulation.

Next, we assessed subjects' attitudes and opinions on data privacy. Though not the focus of the present paper, this section consisted of us asking participants about what companies either should be allowed to do or are allowed to do with consumer data. These questions focused on data collection, retention, third party sharing, and encryption. We collected responses to a battery of information privacy questions. This data collection allowed us to create a cover story for offering the participant identity theft protection.

Answering these questions took up most of respondents' time. In the last few minutes of the survey, they were exposed to a manipulation designed to assess the effectiveness of dark patterns. The first part of the survey provided us with an appropriate pretext for what followed. Respondents were told to wait while the software calculated their "privacy propensity score." All respondents were then told that based on their responses, our system had identified them as someone with a heightened concern about privacy. As such, we would automatically sign them up to receive a data and identity theft protection plan offered by our corporate partner, the largest and most experienced identity theft prevention and credit monitoring company in the United States. This was our bait and switch.

We told participants that by using the demographic information they had provided at the beginning of the survey, along with their IP address, we had pinpointed their mailing address. Our corporate partner would now provide them with six months of free data protection and credit history monitoring. After the six-month period, they would be billed monthly (though they could cancel at any time). The amount they would be billed varied by condition. Participants in the low stakes condition were told that the monthly fee would be \$2.99, and participants in the high stakes condition were told the fee would be \$8.99 per month.

Participants were then allowed to either accept or decline the data protection program. But the steps that were required to do so varied by the level of the dark pattern manipulation. In the control group condition, we did not include any dark patterns. As such, this condition serves as a baseline to help us establish a ceiling for what percentage of the sample was inherently interested in receiving the identity theft protection.³² Participants could thus either

³⁰ In order to preserve confidentiality, these responses were deleted from the data set and were not analyzed.

³¹ Samuel D. Gosling et al., *A Very Brief Measure of the Big Five Personality Dimensions*, 37 J. RES. PERS., 504, 525 (2003).

³² We refer to this figure as a ceiling in the sense that it likely overestimates demand for the service subjects told our corporate partners were selling. This overestimation arises for at least two reasons. First, respondents were told that they already had been signed up for the service (potentially triggering loss aversion at the prospect of its removal) and second, subjects were told that they would pay nothing for the service for the first six months (potentially triggering hyperbolic discounting and optimism bias about whether their future selves would remember to cancel the service once the free trial period ended). We had also primed them to think a lot about privacy, though it is not clear which way that cut, given our

click “Accept” or “Decline” on the first screen. Regardless of which option they selected, they proceeded to the final stage of the experiment, which is described below.

In the mild dark patterns condition, subjects could either click “Accept and continue (recommended) or “Other options,” and the button that accepted the program was selected by default. We made it easier for users to accept the program (because they did not have to select the button themselves) and harder to decline it (because there was not a straightforward and immediate way to decline, only to see other options). Adding a “recommended” parenthetical is a form of false hierarchy. The parenthetical plausibly triggers a heuristic where consumers encounter recommendations made by a neutral fiduciary elsewhere and may be uncertain as to who is making the recommendation and what the basis for that recommendation is.³³

If subjects selected “Other options,” they were directed to the next screen, which asked them to choose between “I do not want to protect my data or credit history” or “After reviewing my options, I would like to protect my privacy and receive data protection and credit history monitoring.” This question uses confirmshaming as a dark pattern to nudge respondents to accept the program (i.e. their decision to decline the program is framed as not wanting to protect their data).

Next, if subjects did not accept the program, they were asked to tell us why they declined the valuable protection. Several non-compelling options were listed, including “My credit rating is already bad,” “Even though 16.7 million Americans were victimized by identity theft last year, I do not believe it could happen to me or my family,” “I’m already paying for identity theft and credit monitoring services,” and “I’ve got nothing to hide so if hackers gain access to my data I won’t be harmed.” They also could choose “Other” and type in their reason, or choose “On second thought, please sign me up for 6 months of free credit history monitoring and data protection services.” This is another confirmshaming strategy. Additionally, it makes it more onerous for many users to decline rather than accept (because if they did not select one of the sub-optimal options provided, they were asked to type out their reason for declining). Subjects who rejected the data protection plan on this screen were treated as having declined the service, and they advanced to the same final screens that those in the control group also saw.

In the aggressive dark pattern condition, the first and second screens were identical to those in the mild dark pattern condition. Participants attempting to decline the identity theft protection were then told that since they indicated they did not want to protect their data, we would like to give them more information so they could make an informed choice. We asked them to read a paragraph of information about what identity theft is. Participants could either choose “Accept data protection plan and continue” or “I would like to read more information.” They were forced to remain on the page for at least ten seconds before being able to advance, and they were shown a countdown timer during this period. This screen created a significant roach motel. Namely, it obstructed respondents’ ability to decline the program by making it more onerous to decline than accept.³⁴ It also toyed with respondents’ emotions by using vivid,

setup. Because we are more interested in comparing the control group to the dark pattern conditions than we are in estimating the actual unmet demand for an identity theft protection service, this potential overestimation presents no problems for our study.

³³ Gray et al., *supra* note 4, at 7.

³⁴ *Id.* at 6.

frightening language in the text. For example, participants read that identity theft “can damage your credit status, and cost you time and money to restore your good name.”

If respondents chose to read more information (rather than accept the program), the next screen had information about why identity theft matters and what a thief could do with their personal information. The options and countdown timer were the same as the previous screen. A third information screen explained how common identity theft is, with the same options and countdown timer displayed before they could advance. The cumulative effect of these screens amounted to a nagging dark pattern.

If participants endured all three information screens and chose “I would like to read more information,” they were then directed to a question designed to confuse them. They were asked, “If you decline this free service, our corporate partner won’t be able to help you protect your data. You will not receive identity theft protection, and you could become one of the millions of Americans who were victimized by identity theft last year. Are you sure you want to decline this free identity theft protection?” The two options were “No, cancel” and “Yes.” This trick question intentionally tried to confuse participants about which option they should select to decline the program.³⁵ Checking the box that includes the word “cancel” counterintuitively accepts the identity theft program. Participants choosing “Yes” were directed to the same last screen as in the mild dark pattern condition, which asked them to indicate their reason for declining the program. After that, they were sent to the same final screens that all subjects saw.

At the conclusion of the study, all participants were asked to indicate their current mood.³⁶ They were then asked whether they would be interested in potentially participating in follow-up research studies by the same researchers.³⁷ Next, they were asked how free they felt they were to refuse the offered plan.³⁸ These questions aimed to assess whether companies that employ dark patterns face any negative repercussions for their use. By comparing the responses of mild and aggressive dark pattern participants to those of the control group we could estimate the size of the good-will loss that a company employing dark patterns would suffer. Lastly, participants were asked how seriously they took the survey, and then were given a text box to write any questions, comments, or concerns they had about the survey. They were then thoroughly debriefed.

A. Rates of Acceptance

The results of the study offer striking empirical support for the proposition that dark patterns are effective in bending consumers’ will. As expected, in the control group condition, respondents opted to accept the identity theft protection program at very low rates. Only 11.3% of respondents accepted the program when they were allowed to accept or decline the program

³⁵ For a discussion of similar dark pattern strategies in Apple’s iOS 6, see WOODROW HARTZOG, *PRIVACY’S BLUEPRINT* 208 (2018).

³⁶ Participants indicated their mood on a scale from 1 (“Happy and relaxed”) to 7 (“Aggravated and annoyed”).

³⁷ Participants indicated their interest on a scale from 1 (“Not at all”) to 7 (“Extremely interested”).

³⁸ Participants indicated their degree of freedom on a scale from 1 (“Not at all free to refuse”) to 7 (“completely free to refuse”).

on the first screen.³⁹ This acceptance rate likely overestimates the demand for a product of this kind.⁴⁰

When mild dark pattern tactics were deployed, the acceptance rate more than doubled. Now 25.8% of participants accepted the data protection program, which corresponds to a 228% increase compared to the control group condition. When participants were exposed to aggressive dark patterns aggressive, the acceptance rate shot up further, with 41.9% of the sample accepting the program.⁴¹ So the aggressive dark pattern condition nearly quadrupled the rate of acceptance, with a 371% increase in rates of acceptance compared to the control group condition. These results are statistically significant and then some. The effect sizes are enormous by the standards of social science research. Manipulative tactics widely employed in the world of brick-and-mortar sales are evidently much less powerful in comparison.⁴²

Table 3: Acceptance Rates by Condition

Condition	Acceptance Rate (%)	Number of Respondents Accepting
Control group	11.3%	73 (out of 644)
Mild	25.8%	155 (out of 600)
Aggressive	41.9%	217 (out of 518)

Given the experimental design, it is possible to determine when participants chose to accept the program in the mild and aggressive dark-pattern conditions. In other words, which of the dark pattern questions seemed to be doing the “work” in nudging participants toward accepting the program? In both conditions, the initial screen (which offered a choice between “Accept and continue (recommended)” and “Other options,” with the former choice pre-selected) accounted for the majority of acceptances. In the mild condition, more than three-quarters of participants who accepted did so on this first screen (75.5%, 117 out of 155). In the aggressive condition, this screen accounted for 65% of acceptances (141 out of 217).⁴³ The

³⁹ Participants were counted as accepting the program if, in any question, they selected the option to accept. They were counted as declining if they indicated they declined in the control group condition, or if they reached the last screen in the mild and aggressive conditions and selected an option other than accepting the program. Therefore, participants who dropped out during the dark pattern manipulation were neither counted as accepting or declining the program. In Table 3 above, if we were to count those who dropped out as decliners, the acceptance rate for the mild dark patterns group would fall to 25% and the acceptance rate for the aggressive dark patterns group would fall to 37%.

⁴⁰ See *supra* note 32.

⁴¹ A chi-square test of independence was performed to examine the relationship between dark pattern condition and acceptance rates. The relation between these variables was significant, $\chi^2(2, N=1762)=142.16, p<.001$.

⁴² See, e.g., Hanson & Kysar, *supra* note 3, at 1447-48 (noting that clever strategies designed to increase impulse buying had boosted sales by “at least ten percent” and placing products at eye-level rather than on a low shelf at a grocery store increases toothbrush purchases by 8 percent).

⁴³ Because the aggressive dark pattern subjects had more opportunities to relent and accept the data protection plan later in the survey it makes sense that this percentage is lower. The higher dropout rate of those in the aggressive dark patterns condition, discussed below, is another contributing factor. Counting

second screen (which offered a choice between “I do not want to protect my data or credit history” and “After reviewing my options, I would like to protect my privacy and receive data protection and credit history monitoring”) accounted for 35 more acceptances in the mild condition (23% of overall acceptances) and 22 more in the aggressive condition (10% of acceptances). For those in the aggressive condition, when participants were forced to read three screens of information on identity theft for at least ten seconds per screen, this roach motel and nagging strategy accounted for 19% of acceptances overall. The confusing trick question (offering an “Are you sure you want to decline this free identity theft protection?” prompt with the options “No, cancel” and “Yes.”) was responsible for another 11% of acceptances. Finally, nearly no one who made it to the final, confirmshaming screen (the list of largely bad reasons for declining the service, with one final chance to accept) ended up accepting, either in the mild or aggressive conditions.

Of course, participants only advanced to new screens in the mild and aggressive conditions if they didn’t “fall” for the dark pattern on an earlier screen. As soon as they accepted the program, the dark patterns ceased (as is often the case in the real world). This means that it is not correct to infer the relative strengths of the different dark patterns deployed from the number of acceptances each caused. Dark patterns that were used later in the manipulation are less likely to work by the very fact that people who were most susceptible to dark patterns were no longer in the sample because they already accepted the data protection plan.

That said, the information about when people accepted is informative for two reasons. First, it demonstrates the substantial cumulative power that different kinds of dark patterns can have. Some people who were able to resist certain dark patterns (like roach motels) are still susceptible to falling for others (like confusingly worded questions). Second, this data demonstrates that seemingly minor dark patterns can have relatively large effects on consumer choices. In the control group condition, participants were able to choose “Accept” or “Decline.” Changing these options to “Accept and continue (recommended)” and “Other options,” with the former pre-selected, all by itself, nearly doubled the percentage of respondents accepting the program.⁴⁴

B. The Influence of Stakes

Across the dark pattern conditions, we varied the price point of the program (\$2.99 vs. \$8.99) to see whether higher monetary stakes influenced rates of acceptance. The neoclassical model of economics generally predicts that consumers will be willing to jump over more hurdles in order to save themselves more money. On this account, consumers face a tradeoff between out-of-pocket expenses to be incurred later and annoying wasted time costs to be incurred now. Impatient consumers should therefore be more likely to relent and accept the program when

dropouts as people who declined the data protection plan, 19.2% of subjects in the mild dark pattern condition and 24.2% of subjects in the aggressive dark pattern condition accepted the offer on the first screen. For a full breakdown of acceptance rate by question, see Appendix A.

Our intuition about this data is that a number of consumers have encountered dark patterns in the wild before and they feel that they can surrender to them now or surrender to them later, so they may as well surrender early and save themselves some time. That said, further studies that randomize the order of dark patterns would be necessary to confirm or refute this hypothesis.

⁴⁴ The acceptance rate increased from 11.3% to 20.7% in the combined dark patterns conditions (counting only those users who accepted on the first dark pattern screen).

the costs of acceptance are lower.⁴⁵ Moreover, rational consumers should be more attentive on average when they are asked to pay a higher price for a good or service, and this might make them less prone to mistakes or impulsive decision-making.

On the basis of these neoclassical assumptions one of the authors (who has produced a fair bit of law & economics scholarship) hypothesized that in the high-stakes condition, overall acceptance rates would be lower. Additionally, he predicted that when respondents had more money at stake, they would be less likely to “fall” for the dark patterns employed in the mild and aggressive conditions. The other author (a psychologist) expressed her consistent skepticism about this hypothesis. The predictions suggested by the neo-classical model were not borne out by the data, and the psychologist’s skepticism proved well-founded. Rates of acceptance were not related to stakes.⁴⁶ There were no significant differences between the high- and low-stakes conditions across any of the dark pattern conditions (see Appendix B for acceptance rates broken down by stakes and level of dark pattern).⁴⁷ Tripling the cost of a service had no effect on uptake in this domain. You read that right.⁴⁸

C. Potential Repercussions of Deploying Dark Patterns

The rates of acceptance in the mild and aggressive conditions show that dark patterns are effective at swaying consumer choices. Though only a small percentage of participants were truly interested in the data protection program for its own sake, a much larger percentage decided to accept the program after we exposed them to dark patterns. These results illustrate why dark patterns are becoming more common — because companies know that they are effective in nudging consumers to act against their own preferences. But it is possible that companies experience a backlash by consumers when they use dark patterns. If so, then there would be less concern that dark patterns are the result of market failure, weakening the case for legal intervention. The questions asked immediately after the experiment were designed to get at this question.

First, participants were asked about their mood to assess whether exposure to dark patterns elicited negative emotions. There was an overall effect of the dark pattern manipulation.⁴⁹ While participants in the control group ($M=2.96$, $SD=1.61$) and mild ($M=3.05$,

⁴⁵ One countervailing force consistent with the neoclassical model is that high price can function as a signal of quality. See, e.g., Ayelet Gneezy et al., *A Reference-Dependent Model of the Price-Quality Heuristic*, 51 J. MARKETING RES. 153, 154 (2014). There is obviously a limit to this signaling dynamic, however, which constrains price increases.

⁴⁶ A chi-square test of independence was performed to examine the relationship between stakes (low vs. high) and acceptance rates. The relation between these variables was not significant, $\chi(1, N=1762)=0.76$, $p=.38$.

⁴⁷ Chi-square tests for independence were run separately for each of the dark pattern conditions. There was no significant relationship between stakes and acceptance rates in the control group ($\chi(1, N=644)=2.52$, $p=.11$), mild ($\chi(1, N=600)=0.27$, $p=.61$), or aggressive ($\chi(1, N=518)=0.19$, $p=.66$) conditions.

⁴⁸ One possible explanation for these results is that consumers in the high-stakes condition felt they were getting six months of very valuable data protection for free, whereas those in the low-stakes condition felt they were getting six months of less valuable data protection for free. It is possible that the greater perceived upside of the six month free trial cancelled out the greater perceived downside of paying \$8.99 per month once the trial period ended.

⁴⁹ $F(2,1740)=323.89$, $p<.001$

SD=1.73) conditions reported similar levels of negative affect, participants in the aggressive condition were significantly more upset ($M=3.94$, $SD=2.06$).⁵⁰ These results suggest that if companies go too far and present customers with a slew of blatant dark patterns designed to nudge them, they might experience backlash and the loss of good will. Yet it is notable that the mild dark pattern condition more than doubled the acceptance rate and did not prompt discernable emotional backlash.

At the end of the study, participants had another chance to express their emotions; they were given a box to type any questions, concerns, or comments they might have. We decided to code these responses to see whether, similar to the explicit mood question mentioned above, participants were more likely to spontaneously express anger after having been exposed to the mild or aggressive dark patterns.⁵¹ The pattern of results mirrored those of the explicit mood measure. Participants in the control group and mild conditions did not express anger at different rates. However, participants in the aggressive dark pattern condition were significantly more likely to express anger.⁵²

Taken together, these two mood measures suggest that overexposure to dark patterns can irritate people. Respondents in the aggressive dark pattern condition reported being more aggravated, and were more likely to express anger spontaneously. It is notable that those respondents exposed to the mild dark patterns did not show this same affective response. Though the mild condition very substantially increased the percentage of respondents accepting the data protection program, there were no corresponding negative mood repercussions.

Even though respondents in the aggressive dark pattern condition overall expressed more negative affect (thereby indicating a potential backlash) it is important to understand what is driving this aggravation. Are people who end up accepting or declining the program equally angered by the use of dark patterns? To answer this question, we compared the moods of people who accepted or declined across the dark pattern conditions. There was an overall main effect, such that people who declined the program reported more displeasure ($M=3.50$, $SD=1.99$) than those who accepted the program ($M=3.21$, $SD=1.78$).⁵³ This effect is driven by the aggressive dark pattern condition. Specifically, among people who accepted the program, there was no significant differences in mood across the control group, mild, and aggressive dark

⁵⁰ Post-hoc Tukey HSD tests confirmed that mean differences in the control group and mild conditions were not significant ($p=.63$), but both differed significantly from the aggressive condition ($p<.001$).

⁵¹ Participants who did not write anything, wrote something neutral, or wrote something positive were coded as a 0. Participants who either expressed general anger or anger specifically at the offer of the data protection program were coded as a 1.

⁵² In the control group condition, 36 out of 632 (5.70%) were coded as expressing anger. In the mild condition, the rate was 36 out of 591 (6.09%). In the aggressive condition, it was 66 out of 515 (12.82%). A chi-square test of independence was performed to examine the relationship between dark pattern condition and whether anger was expressed (Yes/No). The relation between these variables was significant, $\chi(1, N=1738)=23.86$, $p<.001$. The control group and mild conditions did not differ significantly from each other ($\chi(1, N=1151)=0.09$, $p<.77$) but both differed significantly from the aggressive condition (control group vs. aggressive: $\chi(1, N=1045)=17.75$, $p<.001$; mild vs. aggressive: $\chi(1, N=1004)=14.86$, $p<.001$).

⁵³ $F(1,1741)=8.21$, $p=.004$.

pattern conditions.⁵⁴ However, among those who declined, respondents in the aggressive dark pattern condition were more aggravated than those in the control group and mild conditions. The latter two conditions did not differ. This suggests that when dark patterns are effective at leading people to a certain answer, there is no affective backlash. Only when participants are forced to resist a slew of dark patterns in order to express their preference do we observe increased aggravation.

In addition to mood, another potential kind of backlash that dark patterns might elicit is disengagement. People might negatively react because they feel pressured, leading them to want to avoid the dark patterns either in the moment or be hesitant to interact with the entity that employed the dark patterns in the future. In the current study, we have two measures that capture this potential disengagement.

First, participants were able to exit the survey at any time, though if they failed to complete the survey they forfeited the compensation to which they'd otherwise be entitled. We therefore can examine whether participants were more likely to drop out of the study in the aggressive versus mild conditions.⁵⁵ We found that respondents were much more likely to drop out and disengage with the study in the aggressive condition.⁵⁶ Only 9 participants dropped out in the mild condition, while 65 dropped out at some point during the aggressive condition. The latter is an unusual, strikingly high dropout rate in our experience, made all the more meaningful by the sunk costs fallacy. Respondents had typically devoted ten minutes or more to the survey before encountering the dark pattern, and by exiting the survey during the dark pattern portion of the experiment they were forfeiting money they may well have felt like they had already earned.⁵⁷

Second, participants were told that some of them might be contacted to do a follow up survey with the same researchers. They were asked if they were potentially interested in participating. We expected participants to be less interested in the follow-up study if they had been exposed to the mild or aggressive dark pattern conditions. The results supported this

⁵⁴ There was a significant interaction between dark pattern manipulation and outcome, $F(5,1737)=15.12$, $p<.001$. Among people who accepted, there was no main effect of dark pattern condition, $F(2,434)=0.62$, $p=.54$. However, among those who declined, there was a main effect, $F(2,1303)=67.02$, $p<.001$. Post-hoc Tukey tests revealed that respondents who declined after being exposed to the aggressive dark pattern condition were significantly more aggravated than those in the control group and mild conditions ($ps<.001$). Respondents who declined in the control group and mild conditions did not differ significantly, $p=.81$.

⁵⁵ Because the control group condition only contained one question, there was no opportunity for participants to drop out in this condition.

⁵⁶ A chi-square test of independence was performed to examine the relationship between dark pattern condition (mild vs. aggressive) and whether participants dropped out or not. The relation between these variables was significant, $\chi(1, N=1192)=47.85$, $p<.001$.

⁵⁷ The dropout rates observed provide highly relevant information about the social welfare costs of dark patterns. A reasonably high percentage of respondents were willing to forfeit real money rather than continuing to incur the costs of declining an unwanted service or running the risk that they would be signed up for a service they did not want. Of course, by closing their browser and stopping the experiment, there was no guarantee that they would avoid the unwanted subscription. We told respondents at the beginning of the experiment that we had already signed them up for the data protection plan using information they had provided at the beginning of the survey.

hypothesis. Dark pattern condition was significantly related to interest in participating in a follow-up survey.⁵⁸ Participants in the control group condition indicated significantly more interest ($M=4.46$, $SD=2.31$) than participants in the mild ($M=4.11$, $SD=2.32$) and aggressive ($M=3.97$, $SD=2.39$) conditions.⁵⁹ However, here the difference between those in the mild and aggressive conditions was not significant.⁶⁰ This is the one measure of customer sentiment where significant differences were observed between the control group and subjects exposed to mild dark patterns.

One potential reason for the disengagement found above is that the more participants were exposed to dark patterns, the more likely they were to feel coerced into accepting the data protection program. To assess this, we asked participants how free they felt to refuse the data protection program. As expected, condition significantly influenced feelings of freedom.⁶¹ Participants in the control group condition felt freer to refuse ($M=6.21$, $SD=1.44$) compared to those in the mild ($M=5.81$, $SD=1.75$) and aggressive ($M=4.74$, $SD=2.26$) conditions.⁶² Interestingly, as the median scores suggest, most respondents felt more free than unfree to refuse the program, even in the aggressive dark pattern condition.

D. Predicting Dark Pattern Susceptibility

Given the strong influence that dark patterns seem to exert on consumer choice, it is important to understand what individual differences might predict susceptibility. Put another way, what kinds of people are more vulnerable to being manipulated by dark patterns?⁶³ To answer this question, we analyzed whether demographic and personality differences predicted acceptance rates across dark pattern conditions.

We first analyzed whether education predicts acceptance of the program and found that it does.⁶⁴ The less educated participants were, the more likely they were to accept the program. The key question, though, is whether the relationship between level of education and likelihood of acceptance varies by dark pattern condition. In the control group condition, education is not significantly related to whether participants accepted or declined.⁶⁵ This means that in the absence of dark patterns, participants with high and low levels of education do not differentially value the offered program. However, when they are exposed to mild dark patterns, participants

⁵⁸ $F(2,1740)=6.99$, $p=.001$.

⁵⁹ Post-hoc Tukey tests revealed that participants in the control group condition differed significantly from both those in the mild ($p=.02$) and aggressive ($p=.001$) conditions.

⁶⁰ $p=.57$.

⁶¹ $F(2,1739)=96.63$, $p<.001$.

⁶² Post-hoc Tukey tests reveal that all three conditions are significantly different from one another, $p_s<.001$.

⁶³ In other contexts, scholars have found that people with fewer financial resources have more difficulty overcoming administrative burdens that people with more resources. See PAMELA HERD & DANIEL P. MOYNIHAN, ADMINISTRATIVE BURDEN: POLICYMAKING BY OTHER MEANS 7-8, 57-60 (2019).

⁶⁴ A logistic regression was performed to ascertain the effects of education on the likelihood that participants accepted the data protection program. Level of education significantly predicted whether participants accepted or declined the program, $b=-.15$, $SE=.04$, $p<.001$, such that participants with greater levels of education were more likely to decline.

⁶⁵ $b=-.11$, $SE=.08$, $p=.17$.

with less education become significantly more likely to accept the program.⁶⁶ A similar pattern of results emerged in the aggressive dark pattern condition.⁶⁷

When controlling for income, the relationship between education and acceptance varies slightly. The results are similar, except that less education no longer predicts acceptance in the aggressive dark pattern condition.⁶⁸ The relationship persists in the mild dark pattern condition with these controls. This pattern of results endures when additional demographic variables are controlled for.⁶⁹ This result further illustrates the insidiousness of relatively mild dark patterns. They are effective, engender little or no backlash, and exert a stronger influence on more vulnerable populations.

Next, we examined whether political ideology predicted acceptance across dark pattern conditions. Mirroring the results of education, in the control group condition political ideology does not predict acceptance.⁷⁰ But in the mild and aggressive conditions, participants who were more conservative were more likely to accept.⁷¹ This pattern of results remains even when demographic differences are controlled for.⁷² The results are interesting, though the effect sizes are not especially large.

Lastly, we examined whether personality traits predicted susceptibility to dark patterns. At the beginning of the survey, participants filled out a personality inventory that measured the Big 5 traits: extraversion, agreeableness, conscientiousness, neuroticism, and openness. Looking across dark pattern conditions, only extraversion and conscientiousness predict acceptance (See Appendix C for full analyses of all five personality traits).⁷³ More extraverted people and less conscientious people are more likely to accept the program. Breaking down these results by dark pattern condition, the relationship between extraversion and conscientiousness remain in the control group and mild conditions.⁷⁴ However, both traits fail to predict behavior (accepting or declining the program) in the aggressive condition. This result is particularly notable, and confusing, for conscientiousness. People who are conscientious tend to be more diligent and careful. One might expect this personality trait to offer insulation from the manipulative effects of dark patterns. Yet when participants are exposed to a slew of dark patterns in the aggressive

⁶⁶ $b = -.19$, $SE = .06$, $p = .002$.

⁶⁷ $b = -.17$, $SE = .06$, $p = .003$.

⁶⁸ Control group condition: $b = -.08$, $SE = .09$, $p = .40$. Mild condition: $b = -.17$, $SE = .07$, $p = .01$. Aggressive condition: $b = -.07$, $SE = .07$, $p = .27$.

⁶⁹ Controls include income, age, gender, and race (white vs. non-white). Control group condition: $b = -.05$, $SE = .10$, $p = .57$. Mild condition: $b = -.18$, $SE = .07$, $p = .01$. Aggressive condition: $b = -.08$, $SE = .07$, $p = .24$.

⁷⁰ $b = .00$, $SE = .07$, $p = 1.0$.

⁷¹ Mild condition: $b = .12$, $SE = .06$, $p = .03$. Aggressive condition: $b = .13$, $SE = .05$, $p = .01$.

⁷² Controls include gender, age, education, income, and race (white vs. non-white). Control group condition: $b = .02$, $SE = .07$, $p = .79$. Mild condition: $b = .13$, $SE = .06$, $p = .03$. Aggressive condition: $b = .15$, $SE = .05$, $p = .007$.

⁷³ Logistic regressions were run controlling for education, income, gender, age, and race to examine the relationship between extraversion ($b = .10$, $SE = .04$, $p = .02$) and conscientiousness ($b = -.16$, $SE = .05$, $p = .001$) on acceptance rates.

⁷⁴ Extraversion only marginally predicts acceptance in the mild condition. See Appendix C.

condition, we do not see different acceptance rates among those who are more or less conscientious.

To summarize the data we have collected and analyzed here, it appears that dark patterns can be very effective in prompting consumers to select terms that substantially benefit firms. These dark patterns might involve getting consumers to sign up for expensive goods or services they do not particularly want, as in our study and several real-world examples discussed in the previous part, or they might involve efforts to get consumers to surrender personal information – a phenomenon we did not test but that also is prevalent in ecommerce.

From our perspective, it's the mild dark patterns tested – like labeling an option that is good for a company's bottom line but maybe not for consumers as "recommended" or by providing initial choices between "Yes" and "Not Now" – that are most insidious. This kind of decision architecture, combined with the burden of clicking through an additional screen, managed to more than double the percentage of respondents who agreed to accept a data protection plan of dubious value, and it did so without alienating customers in the process. As a result, consumers were manipulated into signing up for a service that they probably did not want and almost certainly did not need. More broadly, we can say the same things about the kinds of dark patterns that are proliferating on digital platforms. These techniques are harming consumers by convincing them to surrender cash or personal data in deals that do not reflect consumers' actual preferences and may not serve their interests. There appears to be a substantial market failure where dark patterns are concerned – what is good for ecommerce profits is bad for consumers, and plausibly the economy as a whole. Legal intervention is justified.⁷⁵

We now know that dark patterns are becoming prevalent and they can be powerful. Knowing these things raises the question of whether they are also unlawful (as unfair or deceptive practices in trade). It also implicates the related question of whether consumer assent secured via dark pattern manipulations ought to be regarded as consent by contract law. Finally, if readers conclude that dark patterns ought to be unlawful or ought not to count as valid consumer consent, that conclusion raises a host of implementation issues. Front and center, can the legal system draw stable lines between permissible (and constitutionally protected) commercial persuasion and impermissible dark patterns? We consider those issues in Part III.

III. Are Dark Patterns Unlawful?

There are several plausible legal hooks that could be used to curtail the use of dark patterns in ecommerce. First, the Federal Trade Commission Act restricts the use of unfair or deceptive practices in interstate trade, providing the Commission with a mandate to regulate and restrict such conduct. Second, state unfair competition laws include similar frameworks. Finally, there is a broad question about whether consumer consent that is procured in a process that employs highly effective dark patterns should be voidable, which would entitle consumers to various remedies available under contract law and which could open up liability for firms that engage in various activities (for example, engaging in surveillance or processing biometric information) without having first obtained appropriate consumer consent.

⁷⁵ See Sunstein, *Sludge Audits*, *supra* note 2, at 15.

A. Laws Governing Deceptive and Unfair Practices in Trade

The F.T.C., with its power to combat unfair and deceptive acts and practices under section 5 of the F.T.C. Act, is the most obvious existing institution that can regulate dark patterns. The scope of the F.T.C.'s investigation and enforcement authority covers "any person, partnership or corporation engaged in or whose business affects commerce,"⁷⁶ with some minor exceptions. As such the F.T.C. has the necessary reach to restrict the use of dark patterns across a wide range of industries. Since 1938 the F.T.C. Act has included language prohibiting "unfair or deceptive acts or practices in or affecting commerce."⁷⁷ The scope of the F.T.C.'s reach and the language of the provision remains broad, reflecting Congress's view that it would be challenging to specify *ex ante* all the different forms of behavior in trade that might be problematic. The Judiciary has consistently deferred to the F.T.C.'s interpretation of its mandate, with the Supreme Court holding in *F.T.C. v. Sperry & Hutchinson Co.*, that the F.T.C. Act allows, "the Commission to define and proscribe practices as unfair or deceptive in their effect upon consumers."⁷⁸

In using its authority to restrict deceptive acts or practices affecting commerce, the F.T.C. treats as deceptive any "representation, omission, or practice" that is (a) material, and (b) likely to mislead consumers who are acting reasonably under the circumstances.⁷⁹ Materiality involves whether information presented "is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product."⁸⁰ Any express product claims made by a company are presumptively material.⁸¹ As for the second prong, "the Commission need not find that all, or even a majority, of consumers found a claim implied" a false or misleading statement. Rather, liability "may be imposed if at least a significant minority of reasonable consumers would be likely to take away the misleading claim."⁸² When enforcing the law, the F.T.C. need not show that the defendants intended to deceive consumers. Rather, it will be adequate for the agency to show that the "overall net impression" of the defendant's communication is misleading.⁸³ Thus, a company cannot make an initial series of misstatements and then bury the corrections of those misstatements in a subsequent communication.⁸⁴

Because lawyers have written very little about dark patterns, and because computer scientists writing in the field are largely unaware of developments in the case law, the existing literature has missed the emergence in recent years of numerous F.T.C. enforcement actions that target dark patterns, albeit without using that term. Indeed, many of the key published

⁷⁶ 15 U.S.C. § 46(a).

⁷⁷ Matthew Sawchak & Kip Nelson, *Defining Unfairness in "Unfair Trade Practices"*, 90 N.C.L. REV. 2033 (2012).

⁷⁸ 405 U.S. 233 (1972).

⁷⁹ In the Matter of Cliffdale Assoc., Inc., 103 F.T.C. 110, 1984 WL 565319 (F.T.C. Mar. 23, 1984).

⁸⁰ *F.T.C. v. Cyberspace.com LLC*, 453 F.3d 1196, 1201 (9th Cir. 2006).

⁸¹ *F.T.C. v. Pantron 1 Corp.*, 33 F.3d 1088 (9th Cir. 1994).

⁸² *Fanning v. F.T.C.*, 821 F.3d 164, 170-71 (1st Cir. 2016).

⁸³ *F.T.C. v. E.M.A. Nationwide, Inc.*, 767 F.3d 611, 631 (6th Cir. 2014).

⁸⁴ *Id.* at 633.

opinions postdate Ryan Calo's survey of the law from 2014, in which he found hardly any relevant F.T.C. enforcement actions.⁸⁵

Federal Trade Commission v. AMG Capital Management is the most important of the dark patterns cases, but because it's very recent and flew under the radar when it was decided it has not yet been discussed at all in the legal scholarship.⁸⁶ The dispute involved the F.T.C.'s enforcement action against a payday lender that was using various dodgy tactics to lure customers. The primary defendant, Scott Tucker, ran a series of companies that originated more than \$5 million in payday loans, typically for amounts less than \$1000.⁸⁷ Tucker's websites included Truth in Lending Act (TILA) statements explaining that customers would be charged a finance rate of, say, 30% for these loans. But the fine print below the TILA disclosures mentioned an important caveat. Amidst "densely packed text" especially diligent readers were informed that customers could choose between two repayment options – a "decline to renew" option and a "renewal" option.⁸⁸ Customers who wanted to decline to renew would pay off the payday loan at the first opportunity, provided they gave Tucker's company notice of their intention to do so at least three business days before the loan was due.⁸⁹ On the other hand, customers who opted for "renewal" would accrue additional finance charges, such as an additional 30 percent premium on the loan. After three such renewals, Tucker would impose an additional \$50 per month penalty on top of the accumulated premiums. As the Ninth Circuit explained, a typical customer who opted for the renewal option could expect to pay more than twice as much for the loan as a typical "decline to renew" customer.⁹⁰ So, of course, Tucker's companies made "renewal" the default option and buried information about how to switch to the "decline to renew" option in a wall of text.⁹¹ That was the case even though the TILA disclosures provided the repayment terms under the assumption that a customer opted to decline to renew.

Judge O'Scannlain, writing for the court, was not impressed with Tucker's protestations that his disclosures were "technically correct." In the Court's view, "the F.T.C. Act's consumer-friendly standard does not require only technical accuracy.... Consumers acting reasonably under the circumstances – here, by looking to the terms of the Loan Note to understand their obligations – likely could be deceived by the representations made here. Therefore, we agree with the Commission that the Loan Note was deceptive."⁹² Tucker's web sites employed numerous dark patterns. Renewal option customers were subjected to forced continuity (a costly subscription by default) and a roach motel (avoiding the onerous default is more taxing than submitting to it). And all customers had to overcome hidden costs (the burial of the renewal option's onerous terms in a long wall of text), preselection (making renewal the default), and trick question text (hard-to-understand descriptions of their options) in order to

⁸⁵ Calo, *supra* note 3, at 1002.

⁸⁶ 910 F.3d 417 (9th Cir. 2018).

⁸⁷ *Id.* at 420.

⁸⁸ *Id.* at 422.

⁸⁹ *Id.* at 423.

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² *Id.* at 424.

avoid paying substantially higher fees. Each of these problematic aspects of the web site design was emphasized by the circuit court.⁹³ The court did not need a dark patterns label or experimental data to see how deceptive the individual strategies and their cumulative effect could be. The circuit court affirmed a \$1.27 billion award against Tucker after he lost on summary judgment.

AMG Capital Management isn't the only recent appellate court opinion in which the courts have regarded dark pattern techniques as deceptive trade practices. In *Federal Trade Commission v. LeadClick Media*, the Second Circuit confronted "disguised ad" behavior and false testimonials.⁹⁴ LeadClick was an internet advertising company, and its key customer was LeanSpa, an internet retailer that sold weight-loss and colon-cleanse products.⁹⁵ LeadClick's strategy was to place much of its advertising on web sites that hosted fake news. Many of the advertisements it placed purported to be online news articles but they were in fact ads for LeanSpa's products. The supposed articles included photos and bylines of the phony journalists who had produced the stories extolling the virtues of LeanSpa's products. As the court explained, these "articles generally represented that a reporter had performed independent tests that demonstrated the efficacy of the weight loss products. The websites also frequently included a 'consumer comment' section where purported 'consumers' praised the products. But there were no consumers commenting – this content was invented."⁹⁶ The Second Circuit thought it was self-evident that these techniques were unlawfully deceptive, reaching that conclusion after articulating the applicable legal standard.⁹⁷ Again, the court lacked the vocabulary of dark patterns, and also lacked data about their efficacy, but it still regarded the issue as straightforward. The Second Circuit's decision echoed a First Circuit decision from the same year, *Fanning v. Federal Trade Commission*, in which that court treated a defendant's incorrect implication that content was user-generated as a deceptive practice in trade.⁹⁸

A recent deceptive conduct F.T.C. action against Office Depot is instructive as to the agency's current thinking. In that complaint, the F.T.C. alleged that Office Depot and its corporate partner, Support.com, were falsely informing consumers that their computers were

⁹³ Id. at 422 (noting the densely packed text); 423 (noting that consumers had to take affirmative action to avoid the renewal option and that there would be subsequent renewals after that); 423-424 ("nothing in the fine print explicitly states that the loan's 'renewal' would be the automatic consequence of inaction. Instead, it misleadingly says that such renewal must be 'accepted,' which seems to require the borrower to perform some affirmative action."); 424 (noting that "between the sentence that introduces the decline-to-renew option and the sentences that explain the costly consequences of renewal, there is a long and irrelevant sentence about what happens if a pay date falls on a weekend or holiday").

⁹⁴ F.T.C. v. LeadClick Media, LLC, 838 F.3d 158 (2d. Cir. 2016).

⁹⁵ Id. at 163.

⁹⁶ Id at 163-64.

⁹⁷ Id. at 168. Though it is not relevant to the portions of the opinion cited here, there is some unfortunate sloppiness in the *LeadClick* opinion. In a couple of instances, the opinion conflates unfair and deceptive practices in trade. See, e.g., *id.* at 168 (erroneously stating that a deceptive practices suit must show that the injury to consumers is not reasonably avoidable by the consumers and is not outweighed by countervailing benefits to consumers or to competition, with a statutory citation that explicitly references the law regarding unfair practices, not deceptive practices). The law is clear that these are not elements of deceptive practices claims. See *Cyberspace.Com*, 453 F.3d at 1199 n.2.

⁹⁸ *Fanning*, 821 F.3d at 171-73.

infected with malware and then selling them various fixes for non-existent problems.⁹⁹ Office Depot and Support.com were apparently employing misleading software that convinced consumers to pay money for virus and malware removal services they did not need.

Advertisements and in-store sales associates encouraged customers to bring their computers to Office Depot for free “PC Health Checks.” When a customer did so, Office Depot employees would ask consumers whether they had any of the following four problems with their computer: (1) frequent pop-up ads, (2) a computer that was running slowly; (3) warnings about virus infections, or (4) a computer that crashed frequently.¹⁰⁰ If the answer to any of those questions was yes, the employees were to check a corresponding box on the first screen of the Health Check software. The computers then had their systems scanned by Office Depot employees using the Support.com software. Customers were led to believe that the process of scanning the computers was what generated subsequent recommendations from Office Depot employees about necessary fixes, such as virus and malware removal services. In fact, the scanning process was irrelevant for the purposes of generating such recommendations. The only relevant factors for generating recommendations were the responses to the first four questions that the employee asked the customer.¹⁰¹

Office Depot strongly encouraged its affiliated stores to push customers towards the PC Health Checks and allegedly expected a high percentage (upwards of 50%) of these Health Checks to result in subsequent computer repairs. Various store employees raised internal alarms about the software, noting that it was flagging as compromised computers that were working properly. These internal complaints evidently were ignored at the C-suite level. Eventually a whistle-blower called reporters at a local Seattle television station. The station had its investigative reporters purchase brand new computers straight from the manufacturers and then bring those computers into Office Depot for PC Health Checks. In several cases, the Support.com software indicated that virus and malware removal was needed. Oops. The journalists’ revelation resulted in an F.T.C. investigation and Office Depot quickly pulled the plug on its PC Health Check software. The companies settled with the F.T.C., agreeing to pay \$25 million (in the case of Office Depot) and \$10 million (in the case of Support.com) to make the case go away, albeit with no admission of wrongdoing on the part of either company.¹⁰²

Several aspects of the deception in *Office Depot* resemble dark patterns. The entire computer scanning process was an example of aesthetic manipulation / hidden information designed to make the customer think that something other than their answers to the first four questions (yes, I see annoying pop-up ads) were driving the company’s recommendations about

⁹⁹ Federal Trade Commission v. Office Depot, Complaint for Permanent Injunction and Other Equitable Relief, Case No. 9-19-cv-80431 (S.D. Fla. Mar. 27, 2019), available at https://www.FTC.gov/system/files/documents/cases/office_depot_complaint_3-27-19.pdf.

¹⁰⁰ *Id.* at 10.

¹⁰¹ Note the similarity between Office Depot’s computer scans and our bogus calculation of each subject’s “privacy propensity score” in the experiment.

¹⁰² Federal Trade Commission v. Office Depot, Stipulated Order for Permanent Injunction and Monetary Judgment, Case No. 9-19-cv-80431-RLR (S.D. Fla. Mar. 28, 2019), available at https://www.FTC.gov/system/files/documents/cases/office_depot_stipulated_order_3-29-19.pdf (Office Depot settlement) and https://www.FTC.gov/system/files/documents/cases/office_depot_-_support.com_stipulated_order_3-29-19.pdf (Support.com settlement); Michelle Singletary, *Office Depot and Support.com to Pay \$35 Million to Settle Charges of Tech Support Scam*, WASH. POST, Mar. 28, 2019.

necessary repairs. There is also a clear bait-and-switch component to the allegations against Office Depot – customers thought they were getting a helpful and free diagnostic from a respected retailer. Instead, they were opening themselves up to a deceitful way for Office Depot to upsell services that many customers did not need. This was done via a mediated online interface employed in brick-and-mortar retail outlets.

Critically, in deciding what constitutes a deceptive practice in trade, the fact that many consumers wind up with terms, goods, or services they do not want strongly suggests that the seller has engaged in deception. That is a key take-away from another Ninth Circuit case, *Cyberspace.com*.¹⁰³ In that case, a company mailed personal checks to potential customers, and the fine print on the back of those checks indicated that by cashing the check the consumers were signing up for a monthly subscription that would entitle them to internet access. Hundreds of thousands of consumers and small businesses cashed the checks, but less than one percent of them ever utilized the defendant's internet access service.¹⁰⁴ That so many consumers had been stuck with something they didn't desire and were not using was "highly probative," indicating that most consumers "did not realize they had contracted for internet service when the cashed or deposited the solicitation check."¹⁰⁵ Courts considering F.T.C. section 5 unfairness suits, discussed below, embrace the same kind of evidence and reasoning.¹⁰⁶ By the same logic, if it appears that a large number of consumers are being dark patterned into a service they do not want (as occurred in our experiment) then this evidence strongly supports a conclusion that the tactics used to produce this assent are deceptive practices in trade.

There is less clear case law surrounding the F.T.C.'s use of section 5 from which to construct a profile of what conduct is "unfair." In the overwhelming majority of enforcement actions, companies choose to settle with the Commission, entering into binding settlement agreements, rather than challenge the commission in court or administrative proceedings.¹⁰⁷ In the absence of judicial decisions; however, consent decrees and other F.T.C. publications have guided companies in interpreting the expected standards of behavior and ensuring their continued compliance with the law.¹⁰⁸

In 1980, the F.T.C. laid out the test that is still currently utilized to find an act or practice "unfair." Under this test, an unfair trade practice is one that 1) causes or is likely to cause substantial injury to consumers 2) is not reasonably avoidable by consumers themselves and 3) is not outweighed by countervailing benefits to consumers or competition.¹⁰⁹ This three-part test is now codified in section 5(n) of the F.T.C. Act.

Generally, the "substantial injury" prong focuses on whether consumers have suffered a pecuniary loss. Monetary harm can come from the coercion of consumers into purchasing

¹⁰³ 453 F.3d at 1196.

¹⁰⁴ *Id.* at 1199.

¹⁰⁵ *Id.* at 1201.

¹⁰⁶ See, e.g., *F.T.C. v. Direct Benefits Group, LLC*, 2013 WL 3771322, Case No. 6:11-cv-1186-Orl-28TBS, at *14 (M.D. Fla. July 18, 2013).

¹⁰⁷ Daniel J. Solove & Woodrow Hartzog, *The F.T.C. and the New Common Law of Privacy*, 114 *COL. L. REV.* 583 (2014).

¹⁰⁸ *Id.*

¹⁰⁹ F.T.C. Policy Statement on Unfairness, 104 F.T.C. 949 (1984).

unwanted goods, or other incidental injuries that come as a result of the unfair action such as financial harm from identity theft. Notably, a harm's substantiality can derive from its collective effect on consumers, as the F.T.C. notes "an injury may be sufficiently substantial, however, if it does a small harm to a large number of people."¹¹⁰

The next prong of the three-part unfairness test is that the injury must not be one that the consumer could have reasonably avoided. This prong is grounded in the belief that the market will be self-correcting and that consumers will learn to avoid companies that utilize unfair practices. Those practices that "prevent consumers from effectively making their own decisions," run afoul of this prong, even if they merely hinder free market decisions, and fall short of depriving a consumer of free choice. For reasonable consumers to avoid harm, particularly in the case of a nonobvious danger, they must also be aware of the possible risk.

The cost-benefit analysis prong of the unfairness test ensures that companies are only punished for behaviors that produce "injurious net effects." There are, as the Commission notes, inevitable trade-offs in business practices between costs and benefits for consumers, and as such certain costs may be imposed on consumers, provided they are balanced by legitimate benefits. Broader societal burdens are also accounted for in this equation, as are the potential costs that a remedy would entail. Additionally, the Commission looks to public policy considerations as part of this analysis to help establish the existence and weight of injuries and benefits that are not easily quantified.

A few cases that resemble dark pattern conduct were brought on unfairness grounds as well as deception. A number of these F.T.C. cases involve unsavory billing practices. One example is *F.T.C. v. Bunzai Media Group, Inc.*, a case in which the F.T.C. secured a settlement of upwards of \$73 million after alleging both deceptive and unfair practices.¹¹¹ In that case the F.T.C. asserted that the defendants' skin-care companies were using a host of dark patterns, including deceptive pop-up ads that stopped consumers from navigating away from a web site without accepting an offer, small print at the very end of a transaction that were in tension with marketing claims used in larger, bold print, and pricing plans that quickly converted "risk-free trials" into renewing monthly subscriptions and were onerous to cancel.¹¹² The F.T.C.'s more recent suit against Triangle Media involved some similar sales tactics, plus a nasty surprise – at the end of the transaction to set up the "free trial," the defendants used misleading web site text to create the false impression that the transaction was not complete until customers signed up for a second free trial for an entirely different product, and they would be signed up for costly monthly subscriptions to both by clicking on the "complete checkout" button.¹¹³ This case too was brought under both prongs of section 5 – deception and unfairness.

¹¹⁰ *Id.*

¹¹¹ 2016 WL 3922625, at *5, Case No. CV 15-4527-GW(PLAx) (C.D. Cal. July 19, 2016).

¹¹² *F.T.C. v. Bunzai Media Group*, Case No. CV 15-4527-GW(PLAx), First Amended Complaint for Permanent Injunction and Other Equitable Relief, (C.D. Cal. Oct. 9, 2015), available at <https://www.FTC.gov/system/files/documents/cases/151009bunzaicmpt.pdf>

¹¹³ *F.T.C. v. Triangle Media Corp.*, 2018 WL 4051701, Case No. 18cv1388-MMA (NLS) (S.D. Cal. Aug. 24, 2018).

F.T.C. v FrostWire, LLC,¹¹⁴ is another case involving alleged unfairness as well as deception, this time with respect to the default settings of a peer-to-peer file sharing service that caused users to share more media than they were lead to believe. The F.T.C. pointed to the obstructionist defaults of the program, which made it exceptionally burdensome for a consumer to prevent all of her files from being shared. As described in the complaint "a consumer with 200 photos on her mobile device who installed the application with the intent of sharing only ten of those photos first had to designate all 200 ... as shared, and then affirmatively unshare each of the 190 photos that she wished to keep private." This user interface presents a classic roach motel employing preselection.

These cases notwithstanding, there is little case law discussing unfairness and dark patterns in depth, especially in comparison to the development of the deceptive acts and practices precedents. Worse still, the leading appellate unfairness case is a Ninth Circuit unpublished disposition that lacks precedential value. The court concluded in that case, for example, that it was unfair conduct for material language to appear in blue font against a blue background on an "otherwise busy" web page.¹¹⁵

Many of the dark patterns discussed earlier could be characterized in a manner to frame the injury as a consumer entering into a transaction they otherwise would have avoided, therefore falling squarely into the current conception of substantial injury. That said, there may be hurdles in conceptualizing dark patterns in a way that fulfills the "unavoidability" prong. When the use of dark patterns is extreme, capitalizing on consumer cognitive bias to the extent that it can be shown to overwhelm their ability to make a free decision, there should be no problem satisfying this prong. At first blush, the milder the use of dark patterns, the more difficult it will be to characterize the harm as unavoidable, particularly when not applied to any exceptionally vulnerable subsets of consumers. On the other hand, our data suggests that milder dark patterns are – if anything – harder to avoid, because of their potent combination of subtlety and persuasive ability.

To summarize, there is an emerging body of precedent in which the federal courts have viewed the F.T.C. as well within its rights to pursue companies that deploy dark patterns online. Among the techniques identified in the taxonomy, false testimonials, roach motels, hidden costs, forced continuity, aesthetic manipulation, preselection, trick questions, and disguised ads have already formed the basis for violations of the F.T.C.'s prohibition on deceptive acts in trade. Techniques that also employ deception, such as false activity messages, sneaking into the basket, bait and switch, forced registration, and scarcity techniques would seem to fall straightforwardly within the parameters of the existing law. Other techniques, like nagging,

¹¹⁴ Complaint for Permanent Injunction and Other Equitable Relief, Oct. 7, 2011, available at 2011 WL 9282853.

¹¹⁵ *F.T.C. v. Commerce Planet, Inc.*, 642 Fed.Appx. 680, 682 (9th Cir. Mar. 3, 2016). The district court's opinion, which is published, and which was affirmed in this respect by the Ninth Circuit, provides more detail. See *F.T.C. v. Commerce Planet, Inc.*, 878 F. Supp.2d 1048, 1066 (C.D. Cal. 2012) ("As placed, the disclosure regarding OnlineSupplier's negative option plan is difficult to read because it is printed in the smallest text size on the page and in blue font against a slightly lighter blue background at the very end of the disclosure. The disclosure is also not placed in close proximity to the 'Ship My Kit!' button and placed below the fold. It is highly probable that a reasonable consumer using this billing page would not scroll to the bottom and would simply consummate the transaction by clicking the 'Ship My Kit!' button, as the consumer is urged to do by the message at the top left: 'You are ONE CLICK AWAY from receiving the most up-to-date information for making money on eBay!'").

price comparison prevention, intermediate currency, toying with emotion, or confirmshaming would probably need to be challenged under section 5's unfairness prong. We were not able to find cases that shed light on whether nagging, toying with emotion, and confirmshaming are lawful. In any event, this survey of the existing precedents suggests that the law restricting dark patterns does not need to be invented; to a substantial degree it's already present.

State unfair competition laws largely track their federal counterpart. There has been far less enforcement activity under these laws targeting dark patterns than there has been under the applicable federal regime. As a result, the law is underdeveloped, and few state cases have broken new ground. An exception is *Kulsea v. PC Cleaner, Inc.*,¹¹⁶ a case brought under California's unfair competition law that predated, and in many ways anticipated, the F.T.C.'s suit against Office Depot. The allegations against PC Cleaner were that the firm's software indicated that there were harmful bugs on the machine that could be addressed via the purchase of the full version of the software.

Another instructive state law case is *In re Lenovo Adware Litigation*.¹¹⁷ That class action case is a sort of split-decision where dark patterns are concerned. Lenovo pre-installed adware on computers that it sold to customers, hiding the software deep within the computers' operating system so it would be difficult to detect and remove. Consumers were given just one chance to remove the software the first time they opened their internet browser, and retaining the software was the default option. Lenovo thus employed preselection, alongside arguable bait-and-switch and hidden costs. A claim brought under New York's consumer protection law, which prohibits deceptive trade practices, was dismissed because the plaintiffs failed to show that they suffered an actual injury, such as a pecuniary harm.¹¹⁸ In the court's view, this lack of pecuniary harm did not justify dismissing the plaintiffs' claims under California state unfair competition law, given that the adware negatively affected the performance of the laptops, and that the installation of the adware was peculiarly within Lenovo's knowledge, material, and a fact that went undisclosed to consumers.¹¹⁹ The case ultimately settled for more than \$8 million.¹²⁰

B. Other Relevant Federal Frameworks

Some enforcement efforts that target dark patterns could be done through the Consumer Financial Protection Bureau (C.F.P.B.), which has the authority to regulate "abusive conduct," at least within the banking and financial services sector. The C.F.P.B. abusive conduct definition is arguably more expansive than the unfair conduct that can be regulated by the F.T.C. An abusive practice, per 12 U.S.C. § 5531 is one that:

¹¹⁶ 2014 WL 12581769, NO. CV 12-0725 FMO (ANx), (C.D. Cal. Feb. 10, 2014).

¹¹⁷ 2016 WL 6277245 (N.D. Cal. Oct. 27, 2016).

¹¹⁸ *Id.* at *10.

¹¹⁹ *Id.* at *11-*14.

¹²⁰ *In re Lenovo Adware Litigation*, 2019 WL 1791420, at *6 Case No. 15-md-02624-HSG (N.D. Cal. Apr. 24, 2019).

(1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or

(2) takes unreasonable advantage of -

(A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;

(B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or

(C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.

This provision would seemingly cover the exploitation of the cognitive biases of consumers in order to manipulate them into making a decision that may not be in their best interests.

Another relevant federal law is the Restore Online Shoppers' Confidence Act (ROSCA).¹²¹ ROSCA makes it unlawful for a third party seller to charge customers absent a clear and conspicuous disclosure of the transaction's material terms, informed consent, and an affirmative step by the consumer indicating willingness to enter into the transaction with the third party.¹²² This law was aimed at the problem of consumers unwittingly being signed up for a subscription to a third party's good or service immediately after entering into a desired transaction with a vendor, where the third party would use the payment information that the consumer had already inputted. The F.T.C. enforces ROSCA in a manner similar to its section 5 enforcement, and ROSCA squarely addresses certain types of bait-and-switch dark patterns, which often employed hidden costs and forced continuity schemes.

C. Contracts and Consent

In his 2018 book, Woodrow Hartzog advanced the argument that contractual consent secured via pernicious forms of dark patterns or other deceptive designs should be deemed invalid as a matter of law.¹²³ Hartzog's argument is built on a series of powerful anecdotes, and the eye-opening data we present here buttresses his bottom line. In our view, Hartzog has it mostly right. The hard part, however, is determining how to tell whether a dark pattern is egregious enough to disregard a consumer's clicking of an "I agree" button. Hartzog's book spends just a few pages developing that particular argument, so there is more theoretical and doctrinal work to be done.

The law's deference to contractual arrangements is premised on a belief that private ordering that commands the mutual assent of the parties makes them better off than the alternative of mandatory rules whose terms are set by the government. The more confidence we have that a contractual arrangement is misunderstood by one of the parties and does not serve the expressed interests of that party, the less reason there is to let the terms of a relationship be set by contract law. To put matters in terms of an influential argument recently

¹²¹ 15 U.S.C. §§8401-05.

¹²² 15 U.S.C. § 8402.

¹²³ HARTZOG, *supra* note 35, at 212-13.

advanced by Rob Kar and Peggy Radin, assent procured mostly via the use of dark patterns doesn't form contracts; it forms pseudo-contracts.¹²⁴ Those shouldn't bind the signatories.

At first blush, hostility to consent induced by dark patterns does not appear to be the direction that the contracts case law has been going of late, though a large part of the problem may be the absence of evidence like the data that our study reveals. *Williams v. Affinion Group, LLC*,¹²⁵ is a key recent case. In *Williams* a confusing user interface was employed by the defendant, Trilegiant, to sign up consumers for membership club purchases while consumers were in the process of shopping for goods and services on sites like Priceline.com.¹²⁶ The consumers were given a discount on their Priceline purchase if they signed up for a membership in one of the defendant's clubs, and if they did so they would be billed \$10 to \$20 monthly for said membership until the consumer cancelled it.¹²⁷ As the Second Circuit described it:

To snare members, Trilegiant allegedly designs its enrollment screens to appear as confirmation pages for the legitimate, just-completed transaction, so that the customer is unaware of having registered to buy and new and completely different product. Trilegiant's cancellation and billing process allegedly prolongs the fraud. To cancel a subscription, the customer must first discover the monthly billing on a credit card statement and call Trilegiant's customer service; Trilegiant's representatives then attempt to keep members enrolled as long as possible, either through promotion of the program's benefits or delay in the cancellation process.¹²⁸

To be clear, not everything described above is a dark pattern, but some of those steps – the disguised ad, the roach motel, the forced continuity, and the nagging – would qualify. The district court's opinion helpfully reproduced the text of Trilegiant's user interface, albeit with much of the text too small to read.¹²⁹ From that text and the lower court opinion it appears the plaintiffs were arguing that the deceptive conduct was evident from a glance at the screenshots.

To the *Williams* court, there was insufficient evidence that this conduct vitiated consent. The plaintiffs produced an expert witness, a marketing scholar, who testified that the user interface "was designed to result in purchases of Trilegiant's services without awareness of those purchases,"¹³⁰ and that the disclosures were designed "so that they would not be seen or understood."¹³¹ The plaintiff's also argued that the relevant terms of the program were buried in "miniscule fine print."¹³²

¹²⁴ Robin Bradley Kar & Margaret Jane Radin, *Pseudo-Contract and Shared Meaning Analysis*, 132 HARV. L. REV. 1135, 1192-1201 (2019).

¹²⁵ 889 F.3d 116 (2d. Cir. 2018).

¹²⁶ *Id.* at 117.

¹²⁷ *Id.* at 120.

¹²⁸ *Id.*

¹²⁹ *In re Trilegiant Corp.*, 2016 WL 8114194, at *2 (D. Conn. Aug. 23, 2016).

¹³⁰ *Williams*, 889 F.3d at 123.

¹³¹ *Id.* at 122.

¹³² *Id.* at 122.

The plaintiff made two key mistakes that, from the Second Circuit’s perspective, warranted the district court’s decision to grant the defendant’s summary judgment motion. First, the expert witness does not appear to have presented any data about consumer confusion – his statements about the interface design and Trilegiant’s likely intentions were conclusory and not supported by evidence in the record.¹³³ Second, the plaintiffs did not argue that the plaintiffs were confused as a result of ambiguous language or design.¹³⁴ In short, the *Williams* opinion leaves the door ajar for class action suits against ecommerce firms that employ dark patterns, provided the proof of consumers being confused or tricked into paying for goods and services they do not want employs the kind of rigorous randomization-based testing that we present here.

The contract doctrine of undue influence provides the most promising existing framework for efforts to curtail dark patterns. Under the Restatement (Second) of Contracts, “undue influence is unfair persuasion of a party who is under the domination of the person exercising the persuasion or who by virtue of the relation between them is justified in assuming that that person will not act in a manner inconsistent with his welfare.”¹³⁵ Comment b of the Restatement emphasizes further that the “law of undue influence ... affords protection in situations where the rules on duress and misrepresentation give no relief. The degree of persuasion that is unfair depends on a variety of circumstances. The ultimate question is whether the result was produced by means that seriously impaired the free and competent exercise of judgment. Such factors as the unfairness of the resulting bargain, the unavailability of independent advice, and the susceptibility of the person persuaded are circumstances to be taken into account in determining whether there was unfair persuasion, but they are not in themselves controlling.”¹³⁶ Undue influence renders a contract voidable by the influenced party.¹³⁷

Applying this rubric, it should not be controversial to assert that packages of dark patterns like the ones employed in our experiment seriously impaired the free and competent exercise of judgment. That seems to be their purpose and effect, as our data show. The harder doctrinal question is whether a consumer and the typical firm that employs dark patterns establishes satisfies either the domination or relationship part of the Restatement test.

The case law suggests that some courts construe the relationship language broadly. In one prominent case, a chiropractor convinced his patient to sign a form indicating that the

¹³³ *In re Trilegiant Corp.*, 2016 WL 8114194, at *11 n.3.

¹³⁴ *Williams*, 889 F.3d at 123 (“[T]o show that customers may have been misled, the plaintiff must produce evidence that particular statements are deceptive when considered in context. These plaintiffs have not attempted to do so. This is not a case involving confusing text; instead, the plaintiffs’ primary contention is that the appearance of an enrollment offer in the course of a separate e-merchant transaction was itself inherently deceptive because it led customers to believe that Trilegiant’s products were associated with or offered by the e-merchant. . . . [T]he plaintiffs’ theory that misleading enrollment pages deceived them into believing they were enrolling in something other than a discount club membership is entirely inconsistent with the record evidence that individual plaintiffs were unaware they enrolled in anything to begin with.”).

¹³⁵ RESTATEMENT (SECOND) OF CONTRACTS § 177 (1981).

¹³⁶ *Id.* at § 177 comment b.

¹³⁷ *Rich v. Fuller*, 666 A.2d 71, 76 (Maine 1995).

patient would pay for the services in full even if her insurance company elected not to cover them.¹³⁸ When the patient objected, saying that she could not afford to pay out of pocket, the chiropractor told her “that if her insurance company said they would take care of her, they would. He told her not to worry.”¹³⁹ These statements induced the patient to sign. The court granted summary judgment to the chiropractor against the patient’s undue influence claim, and the appellate court reversed. From the appellate court’s perspective, these statements uttered in the context of this medical treatment relationship was enough for a reasonable jury to conclude that undue influence had occurred.¹⁴⁰ The majority brushed aside the concerns of a dissenting judge, who accused the majority of invalidating a contract over “nothing more than the urging, encouragement, or persuasion that will occur routinely in everyday business transactions.”¹⁴¹ Another leading case where the court similarly reversed a summary judgment motion involved a relationship between a widow and her long-time friend who was also an attorney.¹⁴²

In influential publications, Jack Balkin and Jonathan Zittrain have proposed that digital platforms like Facebook, Google, Microsoft, and Amazon should owe fiduciary duties to their customers.¹⁴³ If such a proposal were implemented, then the use of effective dark patterns by these platforms would render any consent procured thereby voidable by the customer. This result follows because the law generally presumes undue influence in those instances where a fiduciary owes a duty to a client and the fiduciary benefits from a transaction with its client.¹⁴⁴

Even without embracing Balkin and Zittrain’s information fiduciary theory,¹⁴⁵ dark patterns could be voidable under the domination theory referenced in the Restatement. There is some fuzziness around the precise meaning of domination in the case law. Circumstantial evidence is plainly adequate to prove undue influence.¹⁴⁶ A classic undue influence case describes domination as a kind of “overpersuasion” that applies pressure that “works on mental, moral, or emotional weakness to such an extent that it approaches the boundaries of coercion.”¹⁴⁷ As the court emphasized, “a confidential or authoritative relationship between the

¹³⁸ Gerimonte v. Case, 712 P.2d 876 (Wash. App. 1986).

¹³⁹ Id. at 877.

¹⁴⁰ Id. at 879.

¹⁴¹ Id. at 880 (Scholfield, C.J., dissenting).

¹⁴² Goldman v. Bequai, 19 F.3d 666, 669 (D.C. Cir. 1994).

¹⁴³ See Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC, Oct. 3, 2016, available at <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>.

¹⁴⁴ See, e.g., Matlock v. Simpson, 902 S.W.2d 385, 386 (Tenn. 1995). In those situations the fiduciary must demonstrate the substantive fairness of the underlying transaction to defeat a claim of undue influence.

¹⁴⁵ For a critique of Balkin & Zittrain’s proposal see Lina Khan & David Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. ____ (forthcoming 2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341661.

¹⁴⁶ Nichols v. Estate of Tyler, 910 N.E.2d 221 (Ind. App. 2009); In re Cheryl E., 207 Cal. Rptr. 728, 737 (Cal. App. 1984).

¹⁴⁷ Odorizzi v. Bloomfield Sch. Dist., 54 Cal. Rptr. 533, 539 (Cal. App. 1966).

parties need not be present when the undue influence involves unfair advantage taken of another's weakness or distress."¹⁴⁸ In the court's judgment, undue influence could arise when "a person of subnormal capacities has been subjected to ordinary force or a person of normal capacities subjected to extraordinary force."¹⁴⁹ None of the cases suggest that domination requires a certainty that the dominated party will do the dominant party's bidding.

Nearly quadrupling the percentage of consumers who surrender and agree to waive their rights through non-persuasive tactics like nagging, confusion, hidden costs, or roach motels could satisfy the domination test, particularly when those tactics are unleashed against relatively unsophisticated users. Indeed, in trying to determine whether a tactic amounts to undue influence, courts have emphasized factors such as "limited education and business experience"¹⁵⁰ as well as the uneven nature of the exchange in terms of what the party exercising influence gave and received.¹⁵¹ Similarly, the Restatement identifies "the unfairness of the resulting bargain, the unavailability of independent advice, and the susceptibility of the person persuaded" as the relevant considerations.¹⁵² Treating highly effective dark patterns as instances of domination-induced undue influence would amount to an extension of the doctrine, but it's an extension consistent with the purpose of the doctrine. Furthermore, the availability of quantifiable evidence about the effects of particular dark patterns addresses lingering problems of proof that might otherwise make judges skeptical of the doctrine's application. In short, there are sensible reasons to think that the use of dark patterns to secure a consumer's consent can render that consent voidable by virtue of undue influence.

To push the argument further, there are a number of instances in which the existence of consent is necessary in order for the sophisticated party to a transaction to engage in conduct that would otherwise be unlawful. We identify three such statutory frameworks here. The first is electronic communications law. It is unlawful to intercept an electronic communication (such as a phone call or an email) without the consent of the parties to a communication.¹⁵³ Failure to secure consent has given rise to civil suits under this provision of the Electronic Communications Privacy Act and its state law equivalents.¹⁵⁴ There is a strong argument to be made that consent secured via dark patterns is not adequate consent under these statutes, thereby opening up parties that intercept such communications to substantial liability, especially in cases where

¹⁴⁸ *Id.* at 540. Some, though not all, of the factors relevant to identifying overpersuasion are common in certain forms of dark patterns, such as "discussion of a transaction at an unusual or inappropriate time," "insistent demand that the business be finished at once," "the use of multiple persuaders by the dominant side against a single servient party," and "the absence of third-party advisers to the servient party." As the court explained, "[i]f a number of these elements are simultaneously present, the persuasion may be characterized as excessive." *Id.* at 541.

¹⁴⁹ *Id.* at 541.

¹⁵⁰ *Delaney v. Delaney*, 402 N.W.2d 701, 705 (S.D. 1987).

¹⁵¹ *Goldman*, 19 F.3d at 675.

¹⁵² RESTATEMENT (SECOND) OF CONTRACTS § 177 comment b.

¹⁵³ 18 U.S.C. § 2511(2)(d).

¹⁵⁴ See, e.g., *Deal v. Spears*; *In re Yahoo Mail Litigation*, 7 F. Supp.3d 1016 (N.D. Cal. 2014); *In re Google Inc. Gmail Litigation*, 2013 WL 5423918 (N.D. Cal. Sep. 26, 2013) (No. 13-MD-02430-LHK).

large numbers of communications have been intercepted, such as controversies involving automated content analysis of emails.

Illinois' unique Biometric Identification Privacy Act (BIPA) places similar emphasis on the consent requirement. It requires firms that process the biometric information of consumers to obtain their explicit consent before doing so. The Illinois law sets a high threshold for what counts as adequate consent – firms must inform customers of the fact that biometric information is being collected and stored, the reason for collection, use, and storage, and the duration of storage.¹⁵⁵ The law has produced an avalanche of class action litigation, directed at firms that analyze fingerprints, facial geometry in photos, voiceprints, or other biometric information. In the first half of 2019 new class action suits under BIPA were being filed at a rate of approximately one per day.¹⁵⁶ This rate of new class actions is driven in part by the availability of minimum statutory damages under the statute and the determination by the Illinois Supreme Court that it is not necessary to demonstrate an actual injury in order to have standing to sue under the statute in state court.¹⁵⁷ As ecommerce firms increasingly recognize the scope of their potential exposure to BIPA damages, many have done more to provide the disclosure boxes required by the statute. To the extent that they do so via a disclosure or consent-extracting mechanism that employs dark patterns, the courts could well deem those interfaces (and the “consent” produced thereby) inadequate as a matter of law, opening up the firms that employ those mechanisms subject to very significant liability.¹⁵⁸

A relevant, but not heavily utilized, law exists in California as well. That state enacted a law in 2009 that can be used to aim squarely at forced continuity dark patterns. The law would “end the practice of ongoing charging of consumer credit or debit cards or third party payment accounts without the consumers’ explicit consent for ongoing shipments of a product or ongoing deliveries of service.”¹⁵⁹ Recall Sony’s use of a roach motel to substantially thwart the wishes of PlayStation Plus users who wish to avoid a renewing subscription. There is a very plausible argument that Sony’s obstruction scheme, and ones like it, fall short of the explicit consumer consent standard required by California law. Without stretching the meaning of the statute’s words it is easy to imagine significant class action exposure for Sony.

D. Line Drawing

We expect that most readers will have some sympathy for the idea that dark patterns could be so pervasive in a particular context as to obviate consent. But the hard question, and one readers have probably had on their minds as they read through the preceding pages, is “where does one draw the line?” We would readily concede that some dark patterns are too minor to warrant dramatic remedies like contractual rescission, and some do not warrant a

¹⁵⁵ 740 Ill. Comp. Stat. 14/20(2).

¹⁵⁶ See Seyferth Shaw LLP, *Biometric Privacy Class Actions by the Numbers: Analyzing Illinois’ Hottest Class Action Trend*, July 2, 2019, available at <https://www.jdsupra.com/legalnews/biometric-privacy-class-actions-by-the-48938/>.

¹⁵⁷ *Rosenbach v. Six Flags Entertainment Corp.*, ___ N.E.3d ___, available at 2019 WL 323902 (Ill. Jan. 25, 2019).

¹⁵⁸ For a discussion of liability under these provisions of federal and state wiretap acts and BIPA, see Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69 (2016).

¹⁵⁹ Cal. Bus. & Prof. Code § 17600.

regulatory response of any sort. Small dosages of nagging, intermediate currency, toying with emotion, and confirmshaming may be close to benign and could even be mildly beneficial in limited contexts.¹⁶⁰ Policing them aggressively is unlikely to be cost-justified. At the same time, an “I know it when I see it” approach to dark patterns creates uncertainty, notice problems, and raises the specter of unequal enforcement.

We believe there is a better way forward. In our view, a quantitative approach to identifying dark patterns could be workable and offers many of the benefits of bright-line rules in general. More precisely, where the kind of A/B testing that we discuss above reveals that a particular interface design or option set more than doubles the percentage of users who wind up “consenting” to engage in a consumer transaction, the company practice at issue could be deemed presumptively an unfair or deceptive practice in trade. In the scenarios tested in our experiment, both the mild dark patterns and the hard dark patterns made it more likely than not that consumers were electing not to decline a service on the basis of the choice architecture employed rather than on the basis of innate demand for the service at issue. The “more likely than not” standard is widely employed in civil litigation over torts and other kinds of liability, and it could work well in this context too, ideally with the F.T.C. and academics working hand in hand to replicate high-quality research that quantifies the effects of particular manipulations. As a statistical matter, each individual research subject in our study who was signed up for the data protection plan was more likely than not to have done so because of the dark pattern rather than because of underlying demand for the service being offered.

Admittedly, one challenge here is to develop a neutral baseline against which the A/B testing can occur. With respect to straightforward linguistic choices, that sometimes will be easy. It should not be hard to generate consensus around the idea that a simple Yes / No or Accept / Decline prompt is neutral, provided the choices are presented with identical fonts, colors, font sizes, and placement. Things get more challenging when legal decision-makers must determine whether two, three, four, or five options is neutral, and that is an inquiry that is easier to answer with the benefit of data than it is in the abstract. In close cases, dueling experts may testify, and agencies or courts may be called upon to make the same kinds of factual determinations that is the bread and butter of adjudication. Similarly, there may be some challenges in identifying the neutral baseline where aesthetic manipulation is alleged. Here existing practices may help inform rational determinations about how to assess the baseline. Black text on a white background in a common, 12-point font is used widely enough in communication to where a social scientist treating it as a neutral baseline is unlikely to get

¹⁶⁰ Take the nagging example. As any parent of verbal kids can attest, a modicum of nagging is entirely tolerable. When kids nag their parents it conveys an intensity of preferences to parents, who may appropriately choose to relent after realizing (on the basis of the persistent nagging) that the requested food, activity, or toy really is very important to the child. That said, the legal system has long recognized that nagging should have its limits. The college student who asks a classmate out on a date once or maybe twice, only to be rebuffed, is behaving within acceptable bounds. As the requests mount in the face of persistent rejection, the questions can become harassment. See U.S. DEPARTMENT OF EDUCATION, OFFICE FOR CIVIL RIGHTS, REVISED SEXUAL HARASSMENT GUIDANCE: HARASSMENT OF STUDENTS BY SCHOOL EMPLOYEES, OTHER STUDENTS, OR THIRD PARTIES 6 (2001) (“[B]ecause students date one another, a request for a date or a gift of flowers, even if unwelcome, would not create a hostile environment. However, there may be circumstances in which repeated, unwelcome requests for dates or similar conduct could create a hostile environment.”). It is plausible that after the fifth or sixth request to turn on notifications is declined, a commercial free speech claim lodged against a policy that prevents further requests becomes weak enough for the restriction to survive *Central Hudson* scrutiny.

skeptical looks. As graphics take priority over text, however, things become more complicated, and adjudicators will need to be on the lookout for efforts by hack social scientists to reach their desired answers by manipulating the supposedly neutral baseline.

Bright line rules are particularly useful in the context of enforcing section 5 of the F.T.C. Act. The Due Process Clause requires that companies be able to anticipate when they will face legal liability and when they will not.¹⁶¹ Thus, the more clarity exists in section 5, the less likely it becomes that energetic enforcement of the law will conflict with vital constitutional values. Companies are already doing the kind of beta-testing that reveals how effective their interfaces are becoming at changing consumer behavior. To the extent that there is any doubt about a new technique, they can always examine their own design choices and see whether any cross the line.¹⁶²

In short, it would be appropriate for courts to deem instances in which the “more likely than not” test is satisfied as instances in which consumers have not actually consented to the contractual terms at issue and can void the transaction after the fact. To hold otherwise runs the risk of treating consent as a legal fiction, rather than an indication of mutual assent.

In embracing a “more likely than not” rule, we do not mean to rule out the development of multifactor standards that can supplement a rule-based approach. We are not convinced that a “more likely than not” rule is over-inclusive, as long as dark patterns are defined appropriately, but it may be under-inclusive. For example, the “more likely than not” test works very well when the innate preference for a product among consumers stands at 10 or 20%. But when 40 to 50% of consumers would want to sign up for a service or purchase a product, the “more likely than not” test is likely to let too much manipulative conduct survive. In our view, a situation where 40% of consumers opt to buy a service because of innate demand for it and 20% of consumers opt to buy because of a manipulative interface or choice architecture may still be legally problematic. In those settings it will be necessary to develop a standard that supplements the rule we propose.

A multi-factor test for dark patterns that looks to considerations such as (a) evidence of a defendant’s malicious intent or knowledge of detrimental aspects of the user interface’s design, (b) whether vulnerable populations – like less educated consumers, the elderly, or people suffering from chronic medical conditions – are particularly susceptible to the dark pattern, and (c) the magnitude of the costs and benefits produced by the dark pattern would be a good starting point. Evidence about the ex post regret experienced by consumers who found themselves influenced by a dark pattern might be a particularly revealing indicia of the costs. The greater the number of consumers who complained and sought cancellation of a term they didn’t realize they agreed to, or who didn’t utilize a service they found themselves paying for (as the *Cyberspace.com* court indicated),¹⁶³ the greater the presumptive magnitude of the associated harm would be. By the same token, if it turned out that consumers were happy ex post with a good or service that a dark pattern manipulated them into obtaining, this would be

¹⁶¹ The leading recent case addressing this issue is *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d , 236, 249-59 (3d Cir. 2015).

¹⁶² See Omri Ben-Shahar & Lior Jacob Strahilevitz, *Interpreting Contracts via Surveys and Experiments*, 92 N.Y.U. L. REV. 1753, 1822-24 (2017) (encouraging this kind of beta-testing with consumer contract language).

¹⁶³ See *supra* text accompanying notes 103-105.

revealing evidence cutting against liability for the seller. The ends could justify the means for a firm that genuinely was trying to trick consumers for their own good. But here too, (d) experimental evidence about how effective the dark pattern was compared to a neutral choice architecture should be relevant, albeit not dispositive in a multi-factor inquiry. Thus, even the standard we propose would include a sliding scale that is tied to a quantifiable metric.

The “more likely than not” rule also addresses one of the design challenges that legislators seeking to restrict dark patterns have encountered. As we noted at the outset,¹⁶⁴ bipartisan legislation is presently pending in the Senate to prohibit dark patterns. Senate Bill 1084 would treat the activities of any online service with more than 100 million unique users that “design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data” as unfair or deceptive practices in trade.¹⁶⁵ At the same time, the legislation recognizes that this open-ended prohibition may leave a lot of discretion in the hands of the Commission.

To address this problem, the proposed law does two things. First, it encourages the creation of a standard-setting industry body, which “shall develop, on a continuing basis, guidance and bright-line rules for the development and design of technology products of large online operators”¹⁶⁶ And second, it directs this industry body to “define conduct that does not have the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice ... such as ... de minimis user interface changes derived from testing consumer preferences, including different styles, layouts, or text, where such changes are not done with the purpose of obtaining user consent or user data [and] establishing default settings that provide enhanced privacy protection to users or otherwise enhance their autonomy and decision-making ability.”¹⁶⁷ As this language shows, legislative proponents of clamping down on dark patterns are concerned about the line-drawing problem but feel that without industry input the false-positives problem may become intractable. As our data show, that worry is overblown. Dark patterns were developed through A-B testing, and A-B testing can be used to develop relatively clear and predictable rules about what is permissible. As we explain elsewhere, well-designed surveys are reliable measures for measuring consumer preferences too, so differentiating sludges that seek to undermine widespread preferences from nudges that seek to give consumers what they want is pretty straightforward.¹⁶⁸ An industry association will be more prone to capture than the F.T.C. would be, so there is reason to think that the “more likely than not” test we propose here not only offers a clearer rule but also opens up appealing institutional enforcement options. It could be incorporated into any legislation that tries to address dark patterns.

E. Persuasion

A final, tricky, challenge for a systematic effort to regulate dark patterns is to confront the issue of how to deal with variants of dark patterns that may be constitutionally protected.

¹⁶⁴ See *supra* text accompanying note 7.

¹⁶⁵ Deceptive Experiences to Online Users Reduction Act (DETOUR Act), Senate Bill 1084 §3(a)(1)(A), 116th Congress, introduced April 9, 2019, text available at <https://www.congress.gov/bill/116th-congress/senate-bill/1084/text>.

¹⁶⁶ *Id.* at § 3(c)(3)(A).

¹⁶⁷ *Id.* at § 3(c)(3)(B)(i)-(iii).

¹⁶⁸ See Strahilevitz & Luguri, *supra* note 25.

For most types of dark patterns, this is relatively easy – false and misleading commercial speech is not protected by the First Amendment.¹⁶⁹ Returning to our taxonomy of dark patterns, then, this means that regulating several categories of dark patterns (social proof, sneaking, forced action, and urgency) is constitutionally unproblematic. In our revised taxonomy we have been more careful than the existing literature to indicate that social proof (activity messages and testimonials) and urgency (low stock / high demand / limited time messages) are only dark patterns insofar as the information conveyed is false or misleading. If a consumer is happy with a product and provides a favorable quote about it, it isn't a dark pattern to use that quote in online marketing, absent a showing that it is misleadingly atypical. Similarly, Amazon can indicate that quantities of an item are limited if there really are unusually low quantities available and if the restocking process could take long enough to delay the customer's order. But the First Amendment's tolerance for the imposition of sanctions on commercial speech is premised on the false character of the defendant's representations, such as by making false representations about the source of content on the defendant's web site.¹⁷⁰ This is an important point, one that the existing writing on dark patterns sometimes misses.

Obstruction and interface interference present marginally harder issues. That said, in a leading case relatively blatant examples of these tactics have been deemed deceptive practices in trade. As such, the conduct would not receive First Amendment protection.¹⁷¹ But strategies like toying with emotion, as well as confirmshaming, may be hard to restrict under current doctrine given firms' speech interests. There is virtually no legal authority addressing the question of whether commercial speech that satisfies the F.T.C.'s test for unfairness, but is neither misleading nor deceptive, is protected by the First Amendment.¹⁷² The appellate cases that have been litigated recently tend to involve truthful but incomplete disclosures that create a misimpression among consumers, and F.T.C. action in those cases has generally been deemed constitutionally permissible.¹⁷³

Nagging presents perhaps the thorniest type of dark pattern from a First Amendment perspective. CNN's web site employs a nagging dark pattern, one that regularly asks users whether they wish to turn on notifications. There is no question that CNN's core business is protected by the First Amendment. Would a regulation that prevented them from asking consumers to turn on notifications more than once a month, or once a year, infringe on the company's rights as an organization? It would seem not, so long as the rule were implemented as a broadly applicable, content-neutral rule. Here a helpful analogy is to the Federal Do Not Call registry, which applies to newspapers and other speech-oriented entities, but which has withstood First Amendment challenges.¹⁷⁴ Limits on requests to reconsider previous choices

¹⁶⁹ *Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557, 563 (1980).

¹⁷⁰ *Fanning v. F.T.C.*, 821 F.3d 164, 174-75 (1st Cir. 2016).

¹⁷¹ See, e.g., *F.T.C. v. AMG Capital Mgmt., LLC*, 910 F.3d 417 (9th Cir. 2018) (involving autorenewal, hidden costs, forced continuity, aesthetic manipulation, and preselection).

¹⁷² See Jennifer L. Pomeranz, *Federal Trade Commission's Authority to Regulate Marketing to Children: Deceptive vs. Unfair Rulemaking*, 21 HEALTH MATRIX 521, 550-52 (2011).

¹⁷³ See, e.g., *POM Wonderful LLC v. F.T.C.*, 777 F.3d 478 (D.C. Cir. 2015); *Fanning*, 821 F.3d at 164; *ECM BioFilms, Inc. v. F.T.C.*, 831 F.3d 599 (6th Cir. 2017).

¹⁷⁴ See *Mainstream Marketing Servs. Inc. v. F.T.C.*, 358 F.3d 1228, 1236-46 (10th Cir. 2004) (rejecting a First Amendment challenge to the federal do-not-call registry and holding that the registry's limits on

seem likely to survive similar challenges, provided they establish default rules rather than mandatory ones.¹⁷⁵ On the other hand, the do-not-call cases involve communications by firms to individuals with whom they do not have existing relationships. In the case of nagging restrictions, the government would be limiting what firms can say to their customers in an effort to persuade them to waive existing rights, and it could be that this different dynamic alters the legal bottom line.

Given the potential uncertainty over whether nagging and other forms of annoying-but-nondeceptive forms of dark patterns can be punished, the most sensible strategy for people interested in curtailing these dark patterns is to push on the contractual lever. That is, the First Amendment may be implicated by the imposition of sanctions on firms that nag consumers into agreeing to terms and conditions that do not serve their interests. But there is no First Amendment problem whatsoever with a court or legislature deciding that consent secured via those tactics is voidable. At least in the American legal regime, then, while there is a lot to be gained from considering dark patterns as a key conceptual category, there are some benefits to disaggregation and context-sensitivity, at least in terms of thinking about ideal legal responses.

More broadly, the contractual lever may be the most attractive one for reasons that go far beyond First Amendment doctrine. The F.T.C. has brought some important cases, but neither the federal agency nor enforcers of similar state laws can be everywhere. Public enforcement resources are necessarily finite. But consumers, and attorneys willing to represent them in contract disputes, are numerous. The widespread use of dark patterns could open up firms to substantial class action exposure. As a result, for even a few courts to hold that the use of unfair or deceptive dark patterns obviates consumer consent would significantly deter that kind of conduct.

Conclusion

Computer scientists discovered dark patterns about a decade ago, and there is a sense in which what they have found is the latest manifestation of something very old – sales practices that test the limits of law and ethics. There is a lot to be learned from looking backwards, but the scale of dark patterns, their rapid proliferation, the possibilities of using algorithms to detect them, and the breadth of the different approaches that have already emerged means this is a realm where significant legal creativity is required.

That is not to say that legal scholars concerned about dark patterns and the harms they can impose on consumers are writing on a blank slate. In a series of unheralded F.T.C. deception cases, and in a few unfairness enforcement actions to boot, the regulator best positioned to address dark patterns has successfully shut down some of the most egregious ones. Courts have generally been sympathetic to these efforts, intuiting the dangers posed by these techniques for consumers' autonomy and their pocketbooks. But an observer of the court cases comes away with an impression that the judges in these cases are like the blind men in the parable of the elephant. They do not understand the interconnectedness of the emerging strategies, nor does the nature of judging allow them to make comparisons about the most pressing problems and

telemarketing satisfy the *Central Hudson* test); *National Coalition of Prayer, Inc. v. Carter*, 455 F.3d 783, 787-92 (7th Cir. 2006) (rejecting a First Amendment challenge to a similar state law).

¹⁷⁵ That is, if a customer *wants to be* contacted more than the law provides, they would have the right to permit a commercial speaker to do so. This proviso is important to the constitutional analysis, as *Mainstream Marketing* emphasized that the do not call registry merely established a default.

needs. As a result, they have not given serious thought to the hardest problem facing the legal system – how to differentiate tolerable from intolerable dark patterns.

We think of this paper as making three important contributions to a literature that is growing beyond the human-computer interactions field. First and foremost, there is now an academic paper that demonstrates the effectiveness of various dark patterns. That wasn't true yesterday, even if part of our bottom line is an empirical assessment that has been presupposed by some courts and regarded skeptically by others. The apparent proliferation of dark patterns in ecommerce suggests that they were effective in getting consumers to do things they might not otherwise do, and we now have produced rather solid evidence that this is the case. Paradoxically, it appears that relatively subtle dark patterns are most dangerous, because they sway large numbers of consumers without provoking the level of annoyance that will translate into lost goodwill. Obviously there is a lot more experimental work to do, but this is a critical first step. We hope other social scientists follow us into this body of experimental research.

Second, we have shown how the available experimental evidence helpfully points towards a bright line rule that can be employed to address the aforementioned boundary question. We propose a per se rule that treats a dark pattern technique or combination of techniques that more than doubles consumer assent as presumptively unlawful. Our "more likely than not" test is not a panacea – establishing the neutral choice architecture that is to be used as a baseline for comparison is no breeze, and legal judgments about what conduct counts as constitutionally protected "persuasion" must still be made. The per se rule will be underinclusive, and it will need to be supplemented by a standard. Yet we think the test we have proposed is workable and desirable.

Third, though legal commentators have largely failed to notice, the F.T.C. is beginning to combat dark patterns with some success, at least in court. The courts are not using the terminology of dark patterns, and they have been hamstrung by the absence of data similar to what we report here. But they have established some key and promising benchmarks already, with the prospect of more good work to come. Developing a systemic understanding of the scope of the problem, the magnitude of the manipulation that is occurring, and the legal landmarks that constrain what the government can do will only aid that new and encouraging effort.

The problem we identify here is both an old problem and a new one. Companies have long manipulated consumers through vivid images, clever turns of phrase, attractive spokesmodels, or pleasant odors and color schemes in stores. This behavior should worry us a little, but not enough to justify aggressive legal responses. Regulating this conduct is expensive, and the techniques are limited in their effectiveness, especially when consumers have the opportunity to learn from previous mistakes.

The online environment is different. It's perhaps only a difference of degree, but the degrees are very large. Through A-B testing, firms now have opportunities to refine and perfect dark patterns that their *Mad Men*-era counterparts could have never imagined. By running tens of thousands of consumers through interfaces that were identical in every respect but one, firms can determine exactly which interface, which text, which juxtapositions, and which graphics maximize revenues. What was once an art is now a science. As a result, consumers' ability to

defend themselves has degraded. The trend toward personalization could make it even easier to weaponize dark patterns against consumers.¹⁷⁶

Today the law faces a new technology that presents challenges and opportunities. An analogous dynamic has developed recently with partisan gerrymandering and cell tower geolocation. Partisan gerrymandering has been around for a long time, but computing advances in the last several years have made the state-of-the-art techniques precise at a level entirely without precedent, permitting parties to create much greater partisan advantages than they used to be able to. Once the computers became powerful enough, scholars argued that new legal regimes were warranted.¹⁷⁷ But a bitterly divided Supreme Court ultimately disagreed, at least where the federal Constitution is concerned.¹⁷⁸ A similar challenge arose with geolocation, albeit with different results. It had long been settled that police officers could physically tail suspects without a warrant, but when doing just that became trivially expensive, because cell tower records revealed nearly every person's historic whereabouts, scholars said that legal innovation was necessary.¹⁷⁹ And this time the Supreme Court majority agreed with the scholars.¹⁸⁰

The technology of dark patterns has taken a quantum leap forward, rendering cheap and effective corporate tactics that used to be costly and clunky. So we are making a similar kind of argument to those who suggested that gerrymandering and geolocation technologies had upset status quo assumptions in fundamental ways. Manipulation in the marketplace is a longstanding problem, but recent events have made the problem much worse, and the data presented here gives the strongest hint yet of how large the mismatch is between what consumers want and what they are supposedly consenting to. Dark patterns are a problem that is only going to get worse, because consumers do not have the tools to solve the problem for themselves. Judges, legislators, and regulators now have the data they need to decide whether and how to help.

¹⁷⁶ STRAHILEVITZ ET AL., *supra* note 13, at 34-36.

¹⁷⁷ The most prominent such argument is Nicholas O. Stephanopoulos & Eric M. McGhee, *Partisan Gerrymandering and the Efficiency Gap*, 82 U. CHI. L. REV. 831, 868-76, 899-900 (2015).

¹⁷⁸ *Rucho v. Common Cause*, 139 S. Ct. 2484 (2019).

¹⁷⁹ See, e.g., Matthew Tokson, *Knowledge and the Fourth Amendment*, 111 NW. U. L. REV. 139 (2016); Brief of Amici Curiae Empirical Fourth Amendment Scholars in Support of Petitioner, *Carpenter v United States*, No 16-402 (US filed Aug 14, 2017) (available on Westlaw at 2017 WL 3530963) (Strahilevitz signed and was a primary author of that brief).

¹⁸⁰ *Carpenter v. United States*, 138 S Ct 2206 (2018).

Appendix A

Condition	Total	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Description		Accept/Options	Other options	Info 1	Info 2	Info 3	Trick	Reason
Control group	73	73	n/a	n/a	n/a	n/a	n/a	n/a
Mild	155	117	35	n/a	n/a	n/a	n/a	3
Aggressive	217	141	22	11	10	8	24	1

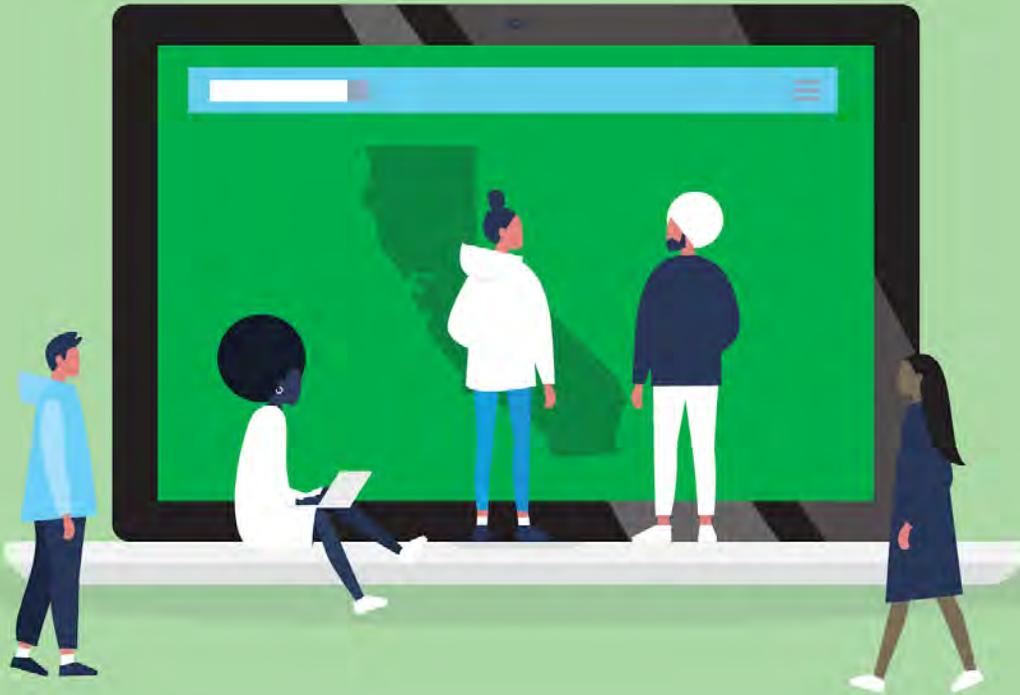
Appendix B

Condition	Overall (% accept)	Low Stakes	High Stakes
Control group	11.3%	9.3%	13.3%
Mild	25.8%	26.8%	24.9%
Aggressive	41.9%	40.9%	42.8%

Appendix C

(When controlling for gender, age, income, race, and education). Numbers represented the beta (standard error).

Trait	Overall	Control group	Mild	Aggressive
Extraversion	.10 (.04) p=.02	.20 (.09) p=.04	.13 (.08) p=.09	.03 (.07) p=.71
Agreeableness	-.09 (.05) p=.08	-.10 (.11) p=.36	-.08 (.08) p=.37	.01 (.09) p=.93
Conscientiousness	-.16 (.05) p=.001	-.29 (.10) p=.006	-.24 (.08) p=.004	-.01 (.08) p=.91
Neuroticism	-.07 (.04) p=.08	-.14 (.09) p=.11	-.04 (.07) p=.54	-.03 (.07) p=.63
Openness	-.05 (.05) p=.29	-.12 (.11) p=.27	-.06 (.08) p=.51	.05 (.08) p=.57



California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

MAUREEN MAHONEY

OCTOBER 1, 2020

Table of Contents

Acknowledgments	3
Executive Summary	4
Introduction	6
Companies' Responsibilities Under the CCPA	8
Methodology	10
Findings	13
Policy Recommendations	44
Conclusion	48
Appendix	49

Acknowledgments

This report is the result of a team effort. Thanks especially to Ben Moskowitz and Leah Fischman for shepherding us through this project, and to Justin Brookman, who provided invaluable assistance throughout. Devney Hamilton, Tom Smyth, and Jill Dimond at Sassafras Tech Collective deserve much of the credit for their work in devising the research study, building the testing tool, and analyzing the results. Kimberly Fountain, Alan Smith, and Daniela Nunez helped us recruit volunteers to participate in the study. Kaveh Waddell made countless contributions and Jennifer Bertsch offered crucial troubleshooting. Karen Jaffe, Camille Calman, Heath Grayson, David Friedman, and Cyrus Rassool improved the report through their review and support. Tim LaPalme and the creative team at Consumer Reports designed the report and helped us present the results more clearly. Finally, our deepest gratitude to the volunteer testers, without whom we would not have been able to conduct this study.

Executive Summary

In May and June 2020, Consumer Reports' Digital Lab conducted a mixed methods study to examine whether the new California Consumer Privacy Act (CCPA) is working for consumers. This study focused on the Do-Not-Sell (DNS) provision in the CCPA, which gives consumers the right to opt out of the sale of their personal information to third parties through a "clear and conspicuous link" on the company's homepage.¹ As part of the study, 543 California residents made DNS requests to 214 data brokers listed in the California Attorney General's data broker registry. Participants reported their experiences via survey.

Findings

- Consumers struggled to locate the required links to opt out of the sale of their information. For 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a "Do Not Sell" link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.
 - Follow-up research focused on the sites in which all three testers did not find the link revealed that at least 24 companies on the data broker registry do not have the required DNS link on their homepage.
 - All three testers were unable to find the DNS links for five additional companies, though follow-up research revealed that the companies did have DNS links on their homepages. This also raises concerns about compliance, since companies are required to post the link in a "clear and conspicuous" manner.
- Many data brokers' opt-out processes are so onerous that they have substantially impaired consumers' ability to opt out, highlighting serious flaws in the CCPA's opt-out model.
 - Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software.
 - Some data brokers asked consumers to submit information or documents that they were reluctant to provide, such as a government ID number, a photo of their government ID, or a selfie.
 - Some data brokers confused consumers by requiring them to accept cookies just to access the site.

¹ Cal. Civ. Code § 1798.135(a)(1).

- Consumers were often forced to wade through confusing and intimidating disclosures to opt out.
- Some consumers spent an hour or more on a request.
- At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.
- At least one data broker used information provided for a DNS request to add the user to a marketing list, in violation of the CCPA.
- At least one data broker required the user to set up an account to opt out, in violation of the CCPA.
- Consumers often didn't know if their opt-out request was successful. Neither the CCPA nor the CCPA regulations require companies to notify consumers when their request has been honored. About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.
- About 52% of the time, the tester was "somewhat dissatisfied" or "very dissatisfied" with the opt-out processes.
- On the other hand, some consumers reported that it was quick and easy to opt out, showing that companies can make it easier for consumers to exercise their rights under the CCPA. About 47% of the time, the tester was "somewhat satisfied" or "very satisfied" with the opt-out process.

Policy recommendations

- The Attorney General should vigorously enforce the CCPA to address noncompliance.
- To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales in one step.
- The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.
- The AG should require companies to notify consumers when their opt-out requests have been completed, so that consumers can know that their information is no longer being sold.
- The legislature or AG should clarify the CCPA's definitions of "sale" and "service provider" to more clearly cover data broker information sharing.
- Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data

minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.

Introduction

California consumers have new rights to access, delete, and stop the sale of their information under the landmark California Consumer Privacy Act, one of the first—and the most sweeping—online privacy laws in the country.² However, as the CCPA went into effect in January 2020, it was unclear whether the CCPA would be effective for consumers. Though the CCPA was signed into law in June 2018, many companies spent most of the 2019 legislative session working to weaken the CCPA.³ Early surveys suggested that some companies were dragging their feet in getting ready for the CCPA.⁴ And some companies, including some of the biggest such as Facebook and Google, declared that their data-sharing practices did not fall under the CCPA.⁵ We suspected that this disregard among the biggest and most high-profile entities would filter down to many other participants in the online data markets, and decided to further explore companies' compliance with the CCPA.

The CCPA's opt-out model is inherently flawed; it places substantial responsibility on consumers to identify the companies that collect and sell their information, and to submit requests to access it, delete it, or stop its sale. Even when companies are making a good-faith effort to comply, the process can quickly become unmanageable for consumers who want to opt out of data sale by hundreds if not thousands of different companies. Given that relatively few consumers even know about the CCPA,⁶

² Cal. Civ. Code § 1798 et seq.; Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (Jun. 28, 2018), <https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>.

³ Press Release, Consumer Reports et al., *Privacy Groups Praise CA Legislators for Upholding Privacy Law Against Industry Pressure* (Sept. 13, 2019), https://advocacy.consumerreports.org/press_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/.

⁴ *Ready or Not, Here it Comes: How Prepared Are Organizations for the California Consumer Privacy Act?* IAPP AND ONETRUST at 4 (Apr. 30, 2019), https://iapp.org/media/pdf/resource_center/IAPPOneTrustSurvey_How_prepared_for_CCPA.pdf (showing that “[M]ost organizations are more unprepared than ready to implement what has been heralded as the most comprehensive privacy law in the U.S. ever.”)

⁵ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, MEDIUM (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>

⁶ *Report: Nearly Half of U.S.-Based Employees Unfamiliar with California Consumer Privacy Act (CCPA)*, MEDIAPRO (Apr. 30, 2019), <https://www.mediapro.com/blog/2019-eye-on-privacy-report-mediapro/>.

participation is likely fairly low. Anecdotally, those that are aware of the CCPA and have tried to exercise their new privacy rights have struggled to do so.⁷ Through this study we sought to get better insight into the challenges faced by consumers trying to exercise their rights under the CCPA's opt-out model.

This study also seeks to influence the regulations implementing the CCPA, to help ensure that they are working for consumers. The CCPA tasks the California Attorney General's office with developing these regulations, which help flesh out some of the responsibilities of companies in responding to consumer requests.⁸ For example, with respect to opt outs, the regulations clarify how long the companies have to respond to opt-out requests⁹ and outline the notices that need to be provided to consumers.¹⁰ On August 14, 2020, the AG regulations went into effect.¹¹ The CCPA directs the AG to develop regulations as needed to implement the CCPA, consistent with its privacy intent,¹² and the AG has signaled that they plan to continue to consider a number of issues with respect to opt outs.¹³

The AG is also tasked with enforcing the CCPA, and this study is also intended to help point out instances of potential noncompliance. Despite efforts of industry to push back the date of enforcement,¹⁴ the AG has had the authority to begin enforcement since July 1, 2020.¹⁵ Already, the AG's staff has notified companies of potential violations of the CCPA.¹⁶

⁷ Geoffrey Fowler, *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST (Feb. 19, 2020), <https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/>.

⁸ Cal. Civ. Code § 1798.185(a).

⁹ Cal. Code Regs. tit. 11 § 999.315(e) (2020).

¹⁰ *Id.* at § 999.304-308.

¹¹ State of California Department of Justice, CCPA Regulations (last visited Aug. 15, 2020), <https://www.oag.ca.gov/privacy/ccpa/regs>.

¹² Cal. Civ. Code § 1798.185(b)(2).

¹³ Cathy Cosgrove, *Important Commentary from Calif. OAG in Proposed CCPA Regulations Package*, IAPP (Jul. 27, 2020), <https://iapp.org/news/a/important-commentary-from-calif-oag-in-proposed-ccpa-regulations-package/>.

¹⁴ See, e.g. Andrew Blustein, *Ad Industry Calls for Delayed Enforcement of CCPA*, THE DRUM (Jan. 29, 2020), <https://www.thedrum.com/news/2020/01/29/ad-industry-calls-delayed-enforcement-ccpa>; Association of National Advertisers, ANA and Others Ask for CCPA Enforcement Extension (Mar. 18, 2020), <https://www.ana.net/blogs/show/id/rr-blog-2020-03-ANA-and-Others-Asks-for-CCPA-Enforcement-Extension>.

¹⁵ Cal. Civ. Code § 1798.185(c).

¹⁶ Cosgrove, *Important Commentary*, *supra* note 13; Malia Rogers, David Stauss, *CCPA Update: AG's Office Confirms CCPA Enforcement Has Begun*, JD SUPRA (Jul. 14, 2020), <https://www.jdsupra.com/legalnews/ccpa-update-ag-s-office-confirms-ccpa-55113/>.

Our study revealed flaws in how companies are complying with CCPA and with the CCPA itself. Many companies are engaging in behavior that almost certainly violates the CCPA. But even if companies were complying completely in good faith, the CCPA makes it incredibly difficult for individuals to meaningfully exercise control over the sale of their personal information. Indeed, the conceit that consumers should have to individually opt out of data sale from each of the hundreds of companies listed on the California data broker registry—let alone the hundreds or thousands of other companies that may sell consumers' personal information—in order to protect their privacy is absurd. Over half of the survey participants expressed frustration with the opt-out process, and nearly half were not even aware if their requests were honored by the recipient. The Attorney General should aggressively enforce the current law to remediate widespread noncompliant behavior, but it is incumbent upon the legislature to upgrade the CCPA framework to protect privacy by default without relying upon overburdened consumers to understand complex data flows and navigate heterogenous privacy controls.

Companies' responsibilities under the CCPA

Under the CCPA, companies that sell personal information (PI) to third parties must honor consumers' requests to opt out of the sale of their PI.¹⁷ The CCPA has a broad definition of personal information, which includes any data that is reasonably capable of being associated with an individual or household—everything from Social Security numbers, to biometric information, or even browsing history. This also covers browsing history or data on a shared computer (in other words, not data that can be exclusively tied to a single individual)¹⁸—further highlighting that opt outs need not be verified to a particular individual. The CCPA's definition of sale covers any transfer of data for valuable consideration,¹⁹ intended to capture data that is shared with third parties for behavioral advertising purposes.²⁰

¹⁷ Cal. Civ. Code § 1798.120(a).

¹⁸ *Id.* at § 1798.140(o)(1).

¹⁹ *Id.* at § 1798.140(t)(1).

²⁰ California Senate Judiciary Committee, SB 753 Bill Analysis at 10 (Apr. 22, 2019), https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200SB753. The analysis excerpts a letter from the sponsors of AB 375, Californians for Consumer Privacy, opposing SB 753, legislation proposed in 2019 that would explicitly exempt cross-context targeted advertising from the CCPA: "SB 753 proposes to amend the definition of "sell" in Civil Code Section 1798.140 in a manner that will break down th[is] silo effect As a result, even if a consumer opts-out of the sale of their data, this proposal would allow an advertiser to combine, share and proliferate data throughout the advertising

The CCPA places certain responsibilities on these companies to facilitate the opt outs. They are required to provide a “clear and conspicuous link” on their homepage so that consumers can exercise their opt-out rights.²¹ The CCPA pointedly creates a separate process for exercising opt-out rights than it does for submitting access and deletion requests—the latter requires verification to ensure that the data that is being accessed or deleted belongs to the correct person.²² In contrast, for opt outs, verification is not required.²³ Importantly, companies may not use the information provided by the opting out consumer for any other purpose.²⁴ The CCPA also directs the AG to design and implement a “Do Not Sell” button to make it easier for consumers to opt out.²⁵

The AG’s regulations outline additional requirements. Companies must post a prominent link labeled “Do Not Sell My Personal Information,” which must lead the consumer to the required interactive form to opt out.²⁶ (The AG declined to finalize a design to serve as an opt-out button.)²⁷ CCPA regulations clarify that “A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request[,]” and the company, if it declines a request for that reason, is required to notify the consumer and provide an explanation.²⁸ Companies must honor consumers’ requests to opt out within 15 business days²⁹ (in contrast to 45 days for deletion and access requests).³⁰

economy. The proposed language will essentially eliminate the silo effect that would occur pursuant to the CCPA, which allows for targeted advertising but prevents the proliferation of a consumer’s data throughout the economy.”

²¹ Cal. Civ. Code § 1798.135(a)(1).

²² *Id.* at § 1798.140(y).

²³ *Id.* at § 1798.135.

²⁴ *Id.* at § 1798.135(a)(6).

²⁵ *Id.* at § 1798.185(a)(4)(C).

²⁶ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

²⁷ State of California Department of Justice, Final Statement of Reasons at 15 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf> [hereinafter FSOR].

²⁸ *Id.* at § 999.315(g).

²⁹ *Id.* at § 999.315(e).

³⁰ Cal. Civ. Code §1798.130(a)(2).

Methodology

In this section, we describe our sample, the research exercise, survey, and method of analysis.

Selecting Companies to Study

To select the companies to study, we used the new California data broker registry,³¹ which lists companies that sell California consumers' personal information to third parties, but do not have a direct relationship with the consumer.³² Reining in data brokers—which profit from consumers' information but typically do not have a direct relationship with them—was a primary purpose of the CCPA. Through the opt out of sale, the authors of the CCPA sought to dry up the pool of customer information available on the open market, disincentivize data purchases, and make data brokering a less attractive business model.³³

The data broker registry was created in order to help consumers exercise their rights under the CCPA with respect to these companies. Companies that sell the personal information of California consumers but don't have a relationship with the consumer are required to register with the California Attorney General each year.³⁴ The AG maintains the site, which includes the name of the company, a description, and a link to the company's website, where the consumer can exercise their CCPA rights.³⁵ The data broker registry is particularly important because many consumers do not even know which data brokers are collecting their data, or how to contact them. Without the data broker registry, exercising CCPA rights with respect to these companies would be near impossible.

For many consumers, data brokers exemplify some of the worst aspects of the ad-supported internet model, giving participants in the study a strong incentive to opt out of the sale of their information. Nearly everything a consumer does in the online or even physical world can be collected, processed, and sold by data brokers. This could

³¹ State of California Department of Justice, Data Broker Registry (last visited August 10, 2020), <https://oag.ca.gov/data-brokers> [hereinafter DATA BROKER REGISTRY].

³² Cal. Civ. Code § 1798.99.80(d).

³³ Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

³⁴ DATA BROKER REGISTRY, *supra* note 31.

³⁵ *Id.*

include location data picked up from apps, purchase history, browsing history—all combined to better understand and predict consumer behavior, and to guide future purchases. Data brokers can purchase information from a variety of sources, both online and offline, including court records and other public documents. The inferences drawn can be startlingly detailed and reveal more about a consumer than they might realize. Consumers can be segmented by race, income, age, or other factors.³⁶ The information collected can even provide insight whether a consumer is subject to certain diseases, such as diabetes, or other insights into health status.³⁷ All of this data might be used for marketing, or it could be used to assess consumers' eligibility for certain opportunities, either due to loopholes in consumer protection statutes such as the Fair Credit Reporting Act, or because of a lack of transparency and enforcement.³⁸

Sampling

We randomly sampled from all of the 234 brokers in California's data broker registry as of April 2020. In the final analysis, we included three sample requests for each of 214 brokers, totaling 642 DNS requests made by 403 different participants. Though we did not have enough testers to ensure that every company on the data broker registry received three tests, a sample of 214 of 234 companies in the database is more than sufficient to represent the different types of processes for all companies. In our initial investigation into DNS requests, in which we submitted our own opt-out requests, we found that three requests were generally enough to uncover the different processes and pitfalls for each company. However, in order to analyze and generalize success rates of DNS requests depending on different processes, a follow-up study should be conducted toward this end. In cases in which testers submitted more than three sample requests for a company, we randomly selected three to analyze.

Participants were not representative of the general population of California. As this initial study was designed to understand the landscape of different data brokers and their DNS request processes, we decided to use a convenience sample. Participants were

³⁶ *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N at 24 (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

³⁷ *Id.* at 25.

³⁸ *Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. at 26 (Mar. 2014), <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>; *Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>.

recruited through CR's existing membership base, promotion by partner organizations, and through social media outreach. Participation was limited to California residents. Therefore, participants were likely better informed about the CCPA and digital privacy rights than the general population. The study was conducted in English, excluding those not fluent in English. Participation in the study was not compensated.

Research Exercise

In the study exercise, participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that data broker. Participants could, and many did, test more than one data broker. On average, participants performed 1.8 test requests. For each request, the participant was given a link to the data broker's website and its email address. They were instructed to look for a "Do Not Sell My Personal Info" (or similar) link on the broker's site and to follow the instructions they found there, or to send an email to the email address listed in the data broker registration if they did not find the link. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker. (See Appendix, Section A for a diagram of the participant experience of the exercise).

Survey Design

The survey aimed to capture a description of a participant's experience in making a DNS request. We approached the design of this study as exploratory to understand the DNS process and as a result, asked mixed qualitative and quantitative questions. The survey branched to ask relevant questions based on what the participant had reported thus far. These questions involved mostly optional multi-select questions, with some open-ended questions. Because the survey included optional questions, not all samples have answers to every question. We omitted from the analysis samples in which there was not enough applicable information for the analysis question. Participants were encouraged to use optional "other" choices with open-ended text. We also offered participants the ability to send in explanatory screenshots. Where participants flagged particularly egregious behaviors, we followed up by having a contractor collect screenshots, or we followed up ourselves to collect screenshots.

Data Analysis

We used both quantitative and qualitative methods for analysis. To answer the questions of time spent and ability to find the DNS request link, we aggregated the responses. To understand the result of request processes, we relied on answers to both open-ended text questions and multi-select questions related to status in order to code and tally the results.

For open response text, we used a qualitative thematic analysis approach where we read the text and coded inductively for themes.

Limitations

This was an exploratory study designed to uncover different DNS processes. As such, our results are not experimental and cannot conclusively establish the efficacy of these DNS processes. Some questions in the survey were meant to capture the participants' experiences, such as "Did the [broker] confirm that they are not selling your data?" For example, a confirmation email could have been sent to the consumer's junk mail folder—so the consumer may not have been aware of the confirmation, even if the company had sent one. Also, consumers may not have understood brokers' privacy interfaces, and conflated DNS requests with other rights; for example, some consumers may have submitted access or deletion requests when they meant to submit opt-out requests. That said, given that the CCPA is designed to protect consumers, consumers' experiences have value in evaluating the CCPA. In addition, because of our convenience sample, it is likely that the broader population may generally drop off from these processes earlier (or not engage at all) due to constraints such as time or lack of technology skill.

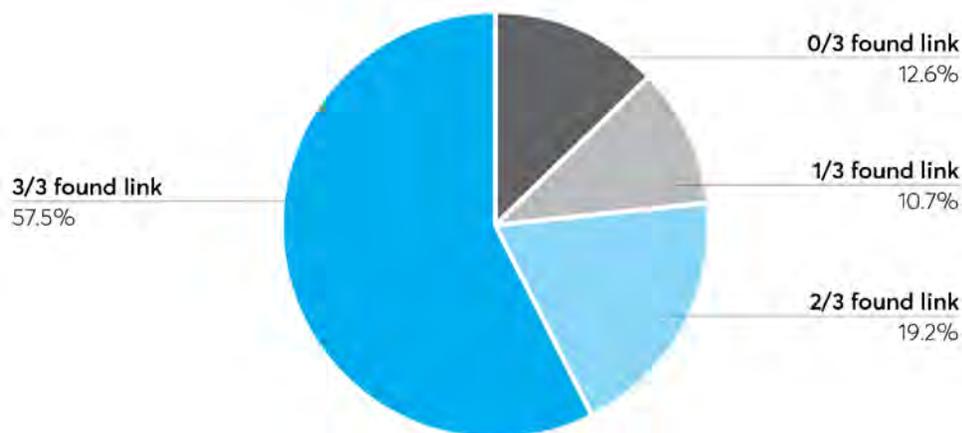
Findings

CCPA opt outs should be simple, quick, and easy. However, we found that many companies failed to meet straightforward guidelines—posing significant challenges to consumers seeking to opt out of the sale of their information. Below, we explore the challenges consumers faced in opting out of the sale of their information from data brokers.

For 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a “Do Not Sell” link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.

Consumers often found it difficult to opt out of the sale of their information, in large part because opt-out links either weren't visible on the homepage or weren't there at all. Nearly half the time, at least one of three of our testers failed to find the link, even though they were expressly directed to look for it. This suggests that either the link wasn't included on the homepage, or that it was not listed in a “clear and conspicuous” manner, both of which are CCPA requirements.

Brokers by number of testers who found DNS link



Companies on the California data broker registry by definition sell customer PI to third parties and should have a Do Not Sell link on their homepage in order to comply with the CCPA. Under California law, every data broker is required to register with the California Attorney General so that their contact information can be placed on the registry.³⁹ A data broker is defined as a “business that knowingly collects *and sells* to third parties the personal information of a consumer with whom the business does not have a direct relationship.”⁴⁰ [emphasis added] The definitions of “sell,” “third parties,”

³⁹ Cal. Civ. Code §1798.99.82.

⁴⁰ *Id.* at § 1798.99.80(d).

and “personal information” all mirror those of the CCPA, which helps to ensure that the registry effectively aids consumers in exercising their CCPA rights with respect to these entities.⁴¹

While it is true that some data brokers may enjoy certain exemptions from AB 1202, companies selling customer information still are obligated to put up Do Not Sell links. In response to requests to the AG during the rulemaking process to “Amend [the CCPA rules] to explain that businesses must provide notice of consumer rights under the CCPA only where such consumer rights may be exercised with respect to personal information held by such business. Consumer confusion could result from explanation of a certain right under the CCPA when the business is not required to honor that right because of one or more exemptions[,]” the AG responded that “CCPA-mandated disclosures are required even if the business is not required to comply with the consumers’ exercise of their rights.”⁴²

The homepage means the first, or landing, page of a website. It is not sufficient to place a link to a privacy policy on the first page, that leads to the DNS link—the link on the homepage must be labeled “Do Not Sell My Personal Information.”⁴³ The CCPA clarifies that “homepage” indeed means “the introductory page of an internet website and any internet web page where personal information is collected.”⁴⁴ The AG further explains that a link to a privacy policy is not sufficient to constitute a Do Not Sell link: “The CCPA requires that consumers be given a notice at collection, notice of right to opt out, and notice of financial incentive. These requirements are separate and apart from the CCPA’s requirements for the disclosures in a privacy policy.”⁴⁵

The CCPA does note that a company need not include “the required links and text on the homepage that the business makes available to the public generally[,]” if it establishes “a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for

⁴¹ *Id.* at § 1798.99.80(e)-(g).

⁴² State of California Department of Justice, Final Statement of Reasons, Appendix A, Response #264 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf> [hereinafter “FSOR Appendix”].

⁴³ Cal. Civ. Code § 1798.135(a)(1).

⁴⁴ *Id.* at § 1798.140(l).

⁴⁵ FSOR Appendix, *supra* note 42, Response #105.

California consumers and not the homepage made available to the public generally.”⁴⁶ We limited our outreach to participants who had previously told us they were California residents, though we cannot say for sure that they were in California at the time they completed our survey. Occasionally California employees supplemented survey responses by capturing additional screenshots, sometimes from within California, sometimes without. Technically, the CCPA gives rights to Californians even when they are not physically present within the state, though it is possible that data brokers treat users differently based on approximate geolocation derived from their IP address.⁴⁷

If testers are unable to find a DNS link on the homepage even if it is there, that suggests that it may not be placed in a “clear and conspicuous” manner, as required by the CCPA. If testers that have been provided instructions and are looking for an opt-out link in order to complete a survey are unable to find a link, it is less likely that the average consumer, who may not even know about the CCPA, would find it.

Testers that did not find an opt-out link but continued with the opt-out process anyway often faced serious challenges in exercising their opt-out rights. We instructed these testers to email the data broker to proceed with the opt-out request. This considerably slowed down the opt-out process, as a consumer had to wait for a representative to respond in order to proceed. And often, the agent provided confusing instructions or was otherwise unable to help the consumer with the opt-out request. For example, we received multiple complaints about Infinite Media. Infinite Media did not have a “Do Not Sell” link on its homepage (see Appendix, Section B for a screenshot). Further, its representative puzzled testers by responding to their opt-out emails with confusing questions—such as whether they had received any marketing communications from the company—in order to proceed with the opt out.

I am with Infinite Media/ Mailinglists.com and have been forwarded your request below. We are a list brokerage company and do not compile any data. We do purchase consumer data on behalf of some of our clients and we do work with a large business compiler and purchase data from them as well. Can you tell me if you received something to your home or business address? If home address I will need your full address info. If business, then please send your company name and address. Also do you work from home? Lastly who was it that you received the mail piece, telemarketing call or email from? I need to know the

⁴⁶ Cal. Civ. Code § 1798.135(b).

⁴⁷ Cal. Civ. Code § 1798.140(g).

name of the company that contacted you so I can track back where the data came from and contact the appropriate list company and have you removed from their data file so they don't resell your name any longer.

Given the number of unsolicited communications that consumers receive, it was difficult for the testers to answer and frustrated their efforts to opt out. One consumer reached out to us after receiving the message: "I don't know how to reply - since I have not received any marketing item from them, ca[n]'t give them the name of outfit/person they're asking about. Our landline does get an annoying amount of robocalls and telemarketing calls but I can't tell who/what they're from...."

The agent's confusing response itself is a potential CCPA violation, as the CCPA requires companies to "[e]nsure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 [regarding the right to opt out] and this section and how to direct consumers to exercise their rights under those sections."⁴⁸ Instead of directing consumers to the interactive form to opt out, the agent confused and frustrated consumers seeking to exercise their CCPA opt-out rights by asking them questions that they could not answer.

At least 24 companies on the data broker registry do not have a DNS link anywhere on their homepages.

Follow-up research on the sites in which all three testers did not find the link revealed that at least 24 companies do not have the required DNS link on their homepage (see Appendix, Section B for screenshots).⁴⁹ For example, some companies provide information about CCPA opt-out rights within its privacy policy or other document, but offer no indication of those rights on the homepage. Since consumers typically don't read privacy policies,⁵⁰ this means that unless a consumer is familiar with the CCPA or

⁴⁸ Cal. Civ. Code § 1798.135(a)(3).

⁴⁹ These companies are: Admarketplace.com, Big Brook Media, Inc., Blue Hill Marketing Solutions, Comscore, Inc., Electronic Voice Services, Inc., Enformion, Exponential Interactive, Gale, GrayHair Software, LLC, Infinite Media Concepts Inc, JZ Marketing, Inc., LeadsMarket.com LLC, Lender Feed LC, On Hold-America, Inc. DBA KYC Data, Outbrain, PacificEast Research Inc., Paynet, Inc., PossibleNow Data Services, Inc, RealSource Inc., Social Catfish, Spectrum Mailing Lists, SRAX, Inc., USADATA, Inc., and zeotap GmbH.

⁵⁰ Brooke Axier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RESEARCH CTR. (Nov. 15, 2019),

is specifically looking for a way to opt out, they likely won't be able to take advantage of the DNS right.

For example, the data broker Outbrain doesn't have a "Do Not Sell My Personal Information" link on its homepage. The consumer can click on the "Privacy Policy" link at the bottom of the page, which sends the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer can cut out several steps by clicking on "Interest-Based Ads" on the homepage.) If a consumer would like to opt out on their phone, they would have to go through another process. And if the consumer clears their cookies, they would need to opt out again. As one consumer told us, "It was not simple and required reading the 'fine print.'" Below, we show the opt-out process through screenshots (See pages 20-21):

STEP 1 The "Privacy Policy" link takes the consumer to the "Privacy Center." Consumers can click on panel 6, "California Privacy Rights," **STEP 2.**

Clicking on "California Privacy Rights" opens up a text box **STEP 3**, that includes a bullet on the "Right to opt-out of the 'sale' of your Personal Information." That section includes a very small hyperlink to "opt out of personalised recommendations."

Clicking on that link takes the consumer to another to a page titled "Your Outbrain Interest Profile," **STEP 4.** (The consumer can also reach this page by clicking on "Interest-Based Ads" on the homepage.)

The consumer can then click on "View My Profile," which takes them to a new page that provides a breakdown of interest categories. In the upper right-hand corner, there is a small, gray-on-black link to "Opt Out," **STEP 5.**

This finally takes the consumer to a page where they can move a toggle to "opt out" of interest-based advertising, **STEP 6**, though it is unclear whether turning off personalized recommendations is the same as opting out of the sale of your data under the CCPA. One tester remarked on the confusion, "There were many links embedded in the Outbrain Privacy Center page. I had to expand each section and read the text and review the links to determine if they were the one I wanted. I am not sure I selected "DO not Sell" but I did opt out of personalized advertising."

<https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/> (Showing that only 9% of adults read the privacy policy before accepting the terms and conditions, and 36% never do.).

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

Outbrain Advertisers Publishers About Us Help Center Blog Careers Contact Us Register

The Open Web's
Discovery & Native Advertising Feed

Advertise with Us Publishers, Let's Talk

Privacy Policy

STEP 1

4. Children
5. European Territory Citizens
6. California Privacy Rights
7. "Do Not Track" Disclosure
8. How This Privacy Policy May Change

STEP 2

- ◆ Right to opt-out of the "sale" of your Personal Information. We do not sell your Personal Information in the conventional sense (i.e., for money). However, like many companies, we use services that help deliver interest-based ads to you. California law classifies our use of these services as a "sale" of your Personal Information to the companies that provide the services. This is because we allow them to collect information from our website users (e.g., online identifiers and browsing activity) so they can help serve ads more likely to interest you.] To opt-out of this "sale," click on [this link](#) which will take you to our Interest Profile where you can opt out of personalised recommendations.

STEP 3

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

Outbrain

Your Outbrain Interest Profile [Interest Profile](#)
Our transparency promise to you

You know the recommendations you see throughout articles you're reading? Ever wonder *how* those recommendations were served to you?

Let us introduce ourselves. We're **Outbrain**. We help you discover the content most interesting to you — content you may not have discovered yet before.

By clicking "View My Profile" below, you'll see just how we tailor these recommendations, based on your truest interests.

VIEW MY PROFILE

STEP 4

Outbrain [Privacy Policy](#) [Contact Us](#) [Opt Out](#)

Your Outbrain Interest Profile [Interest Profile](#)
The below graph is a breakdown of your interest categories.
Click any of the graph sections to take a deeper look.

Website Visits

Opt Out

STEP 5

Our promise to you is transparency and choice.
Select your recommendation settings below:

Personalized Interest Recommendations

Non-Personalized Recommendations (Opt Out)

Mobile Application Opt-Out

Simply update your mobile device settings to opt-out of Outbrain recommendations on your mobile applications.

iOS Devices: Settings > Privacy > Advertising > Limit Ad Tracking

Android Devices: Google Settings App > Ads > Opt Out of Interest-based Advertising

STEP 6

Even those steps don't opt consumers out for all devices. There are separate instructions for opting out on a mobile device, and for bulk opting out of ad targeting through a voluntary industry rubric (though again, it isn't clear if this is the same as stopping sale under the CCPA).

Instead of leaving consumers to navigate through multiple steps to opt out, Outbrain should have included a link that says "Do Not Sell My Personal Information" on the homepage, and then immediately taken the consumer to a page with the toggle to opt out. The AG's regulations require companies to provide "two or more designated methods for submitting requests to opt out, including an *interactive form* accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application."⁵¹ (emphasis added). This suggests that the opt out is intended to involve nothing more than filling out a short form, one that is quickly and easily accessed from the homepage.

For an additional five companies, all three testers were unable to find the DNS link, suggesting that they may not be listed in a "clear and conspicuous" manner as required by the CCPA.

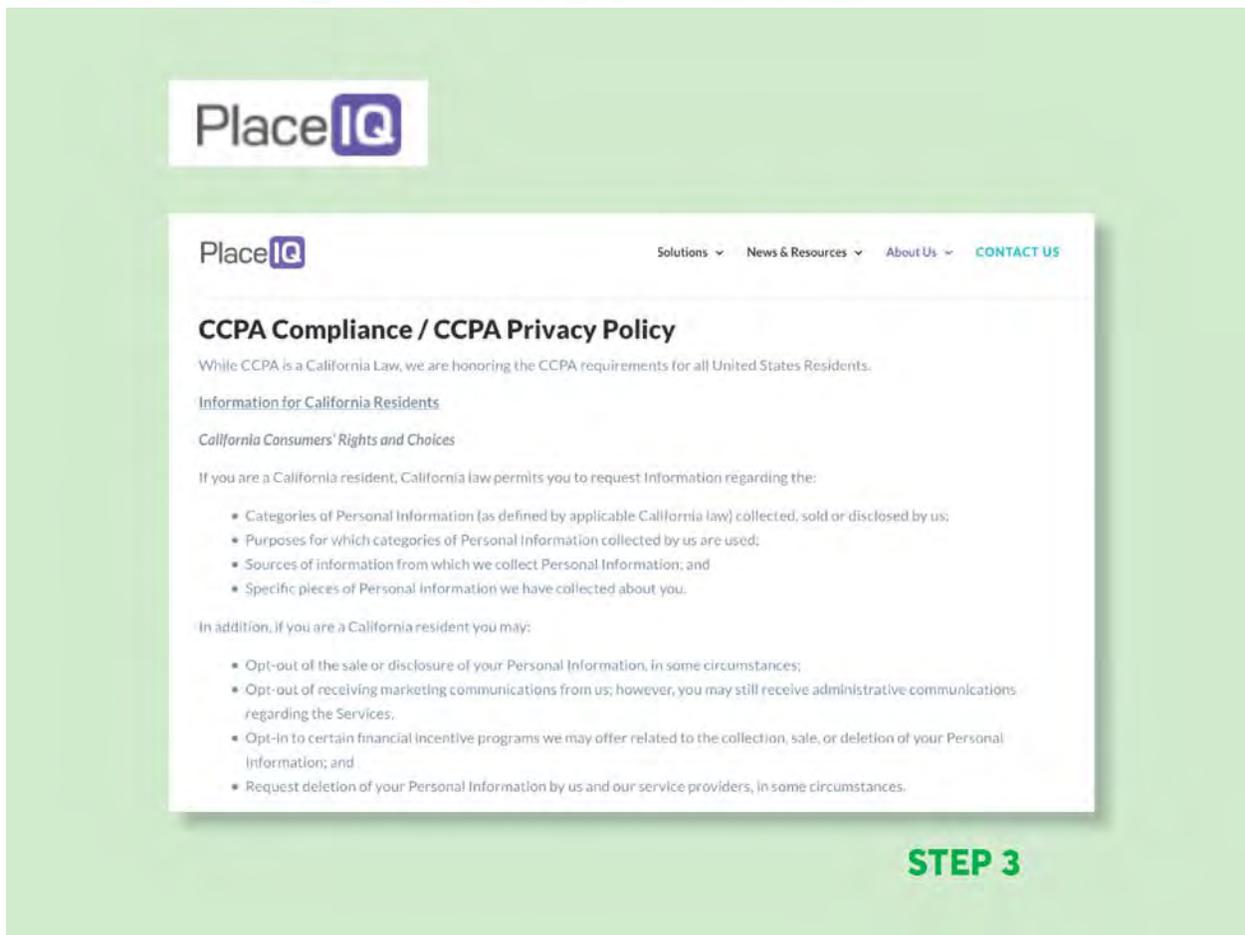
All three testers were unable to find the DNS link for an additional five companies (see Appendix, Section C for screenshots).⁵² For example, all three testers failed to find the Do Not Sell link for the data broker Freckle I.O.T. Ltd./PlacelQ. First, the website <https://freckleiot.com/>, which is listed on the data broker registry, automatically redirects to <https://www.placeiq.com/>, where consumers are confronted with a dark pattern banner at the bottom of the screen that only offers the option to "Allow Cookies" (the banner also states that "scrolling the page" or "continuing to browse otherwise" constitutes consent to place cookies on the user's device.) If the user does not click "Allow," the banner stays up, and it obscures the "CCPA & Do Not Sell" link (for more on mandating cookie acceptance as a condition of opting out, see *infra*, p. 30).

⁵¹ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

⁵² These companies are: AcademixDirect, Inc., Fifty Technology Ltd, Freckle I.O.T. Ltd./PlacelQ, Marketing Information Specialists, Inc., and Media Source Solutions. Two of the companies in which all three testers could not find the DNS link did not appear to have a functioning website at all: Elmira Industries, Inc. and Email Marketing Services, Inc.

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

The image shows a screenshot of the PlaceIQ website with two callouts illustrating steps to find privacy information. **STEP 1** highlights a blue 'Allow cookies' button in a white box, which is part of a dark cookie consent banner at the bottom of the page. The banner also contains text about cookies and another 'Allow cookies' button. **STEP 2** highlights a 'Privacy Policy' link in a green box within the 'Consumer Options' section of the website footer. The footer also lists 'CCPA & Do Not Sell' and includes social media icons and a copyright notice for 2020 PlaceIQ.



After clicking “Allow Cookies,” revealing the full homepage, then, the user must scroll all the way down to the bottom of the homepage to get to the CCPA & Do Not Sell link (also note that the link is not labeled “Do Not Sell My Personal Information” as required by the CCPA).

Since users must accept cookies to remove the pop up and reveal the link, and the link was buried at the very bottom of the page, it is not surprising that none of the consumers testing the site were able to find the opt-out link, even though they were looking for it. This shows how confusing user interfaces can interfere with consumers’ efforts to exercise their privacy preferences, and how important it is for companies to follow CCPA guidance with respect to “clear and conspicuous” links. Without an effective mechanism to opt out, consumers are unable to take advantage of their rights under the law.

Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software, raising serious questions about the workability of the CCPA for consumers.

While companies might need to collect some information from consumers in order to identify consumer records—for example, data brokers typically sell records by email⁵³—some companies asked for information that was difficult to obtain, or required consumers to undergo onerous processes in order to opt out. There were a variety of formats for making DNS requests such as instructions to download a third-party app, instructions to send an email, or no instruction or clearly visible opt-out link at all (we instructed our participants to send an email to the email address in the registry if they could not find the opt-out link).

The most common type of DNS process involved filling out a form with basic contact information such as name, email, address, and phone number. However, several companies, such as those tracking location data, asked consumers to provide an advertising ID and download a third-party app to obtain it. This was confusing and labor intensive for many testers.

Companies that defaulted to pushing consumers to install an app to obtain the ID discouraged some consumers from opting out—downloading a separate app to their phone was a step too far. One tester of data broker Freckle I.O.T./PlacelQ reported, “Too technically challenging and installing an app on your phone shouldn't be required.” The consumer further notes that the Freckle I.O.T./PlacelQ opt-out process would be impossible for consumers without a mobile phone. “The process also could not be completed on a computer, so anyone without a smartphone would not be able to complete the request this way.” In nearly half (8 out of 20) of cases, consumers declined to provide an advertising or customer ID.

Other consumers found themselves unable to submit opt-out requests because the company required an IP address. For example, four testers reported that they could not complete their request to Megaphone LLC because they were asked to provide their IP address. In this case, it was likely that testers declined to proceed further because they could not figure out how to obtain their IP address. The screenshot on page 25 shows that Megaphone’s opt-out form includes a required question, “What is your IP address?”

⁵³ For example, TowerData claims that clients can obtain “data on 80% of U.S. email addresses.” TowerData (last visited Sept. 13, 2020), <http://intelligence.towerdata.com/>.

Megaphone

Megaphone Advertisers Publishers About Press Log in Contact us

Modern podcast technology for publishers and advertisers.

Do not sell my personal information

By using this site, you agree to the use of cookies by Megaphone and our partners to provide the best experience, analyze site use and deliver advertising. [Privacy Policy](#) Close

STEP 1

CCPA Request

California residents may use this form to submit a request to opt out of the "sale" of their personal information to third parties.

The only personal information that Megaphone collects is a user's IP address and user agent, which is information about the user's device, browser, and platform of origin. We require California residents to submit their IP address and the platform from which they download podcasts because, without that information, we have no way to act on their requests.

* Name
[Text Input Field]

* Email address
[Text Input Field]

* What is your IP address?
[Text Input Field]

* What is your user agent?
[Dropdown Menu: -Select-]

I'm not a robot 

SUBMIT

STEP 2

Some data brokers asked consumers to submit information that they were reluctant to provide, such as a photo of their government ID.

Some companies asked consumers to verify their identities or residence, for example by providing their government ID number, an image of their government ID, or a “selfie.” Testers reported that a few asked knowledge-based authentication questions, such as previous addresses or a home where someone has made a payment.

The histogram on page 27 shows the relative frequency of types of information testers were asked for and steps they were asked to take as part of their DNS request.⁵⁴

⁵⁴ All requests are combined in this analysis (rather than broken down by broker), reflecting the overall experience of making DNS requests under the CCPA. For reporting what is asked of testers in the process, we used the answers to multi-select questions about what information testers were asked for and/or refrained from providing, and multi-select questions about actions they were asked to take and/or refrained from taking. As some of the action options were redundant of the information options, we combined a non-repeat subset of the action options with the information options. We also used text answers in these parts of the survey in qualitative analysis about the variety of DNS processes.

DNS Request Processes



A company needs some personal information in order to process a “Do Not Sell” request—if a data broker sells records linked to email addresses, it needs to know the email address about which it is no longer allowed to sell information. Nevertheless,

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

companies are not allowed to mandate identity verification to process a DNS request under CCPA, and requesting sensitive information provided friction and led many consumers to abandon their efforts to opt out. See, for example, the Melissa Corporation, which requested consumers to provide “verification of California residency and consumer’s identity.”

melissa

melissa

California Consumer Privacy Act Notice (Show Details...)

Right to Know

Right to Opt-Out of Sale of Personal Information

Right to Delete

Please provide the information that you want to inquire.

First Name: Last name:

Phone: Mobile Phone:

Email:

Address:

Address2:

City: State: CA ▾

ZIP/Postal Code:

*Attach verification of California residency and consumer's identity (Supported files: .pdf, .jpg, .jpeg, .gif, .bmp, .png, .tif)

Choose File No file chosen

Choose File No file chosen

Choose File No file chosen

Submit

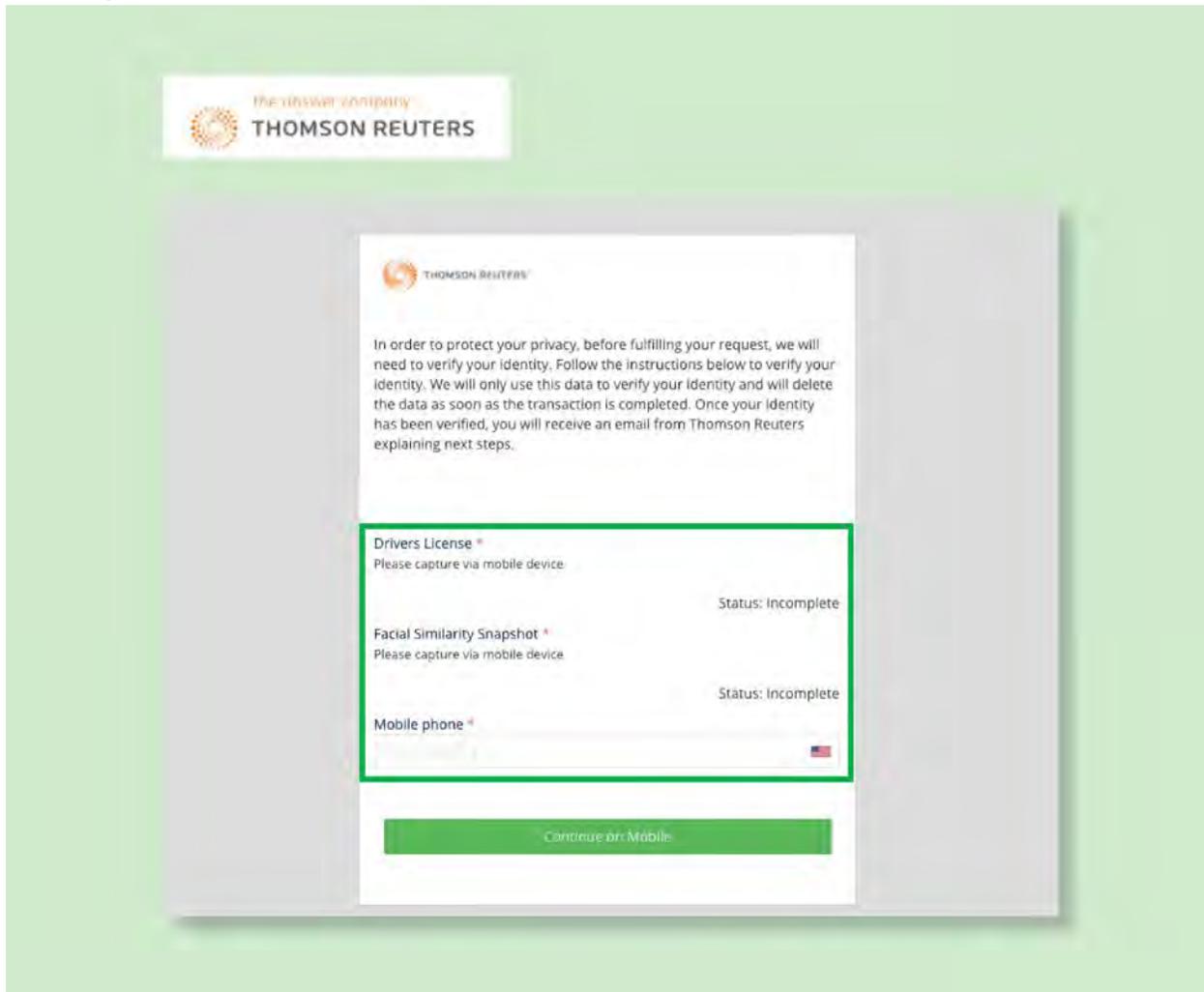
The CCPA only covers California consumers,⁵⁵ and the statute and implementing regulations are ambiguous on how companies may require consumers to prove they are

⁵⁵ Cal. Civ. Code § 1798.140(g).

California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

covered by the law. However, asking for proof of residence added difficulty to the opt-out process, especially as other companies achieved this objective by requesting the consumer's name, address, and email.

West Publishing Corporation, part of Thomson Reuters, also asked consumers to submit to identity verification to complete the opt-out process. As shown in the screenshot below, the site requires consumers to submit a photo of their government ID and a selfie, as well as their phone number. Once the phone number is submitted, the site sends a text to help facilitate the capture of these documents through the user's mobile phone.



While these requests might be appropriate in the case of an access or deletion request, where identity verification is important to make sure that data is not being accessed or

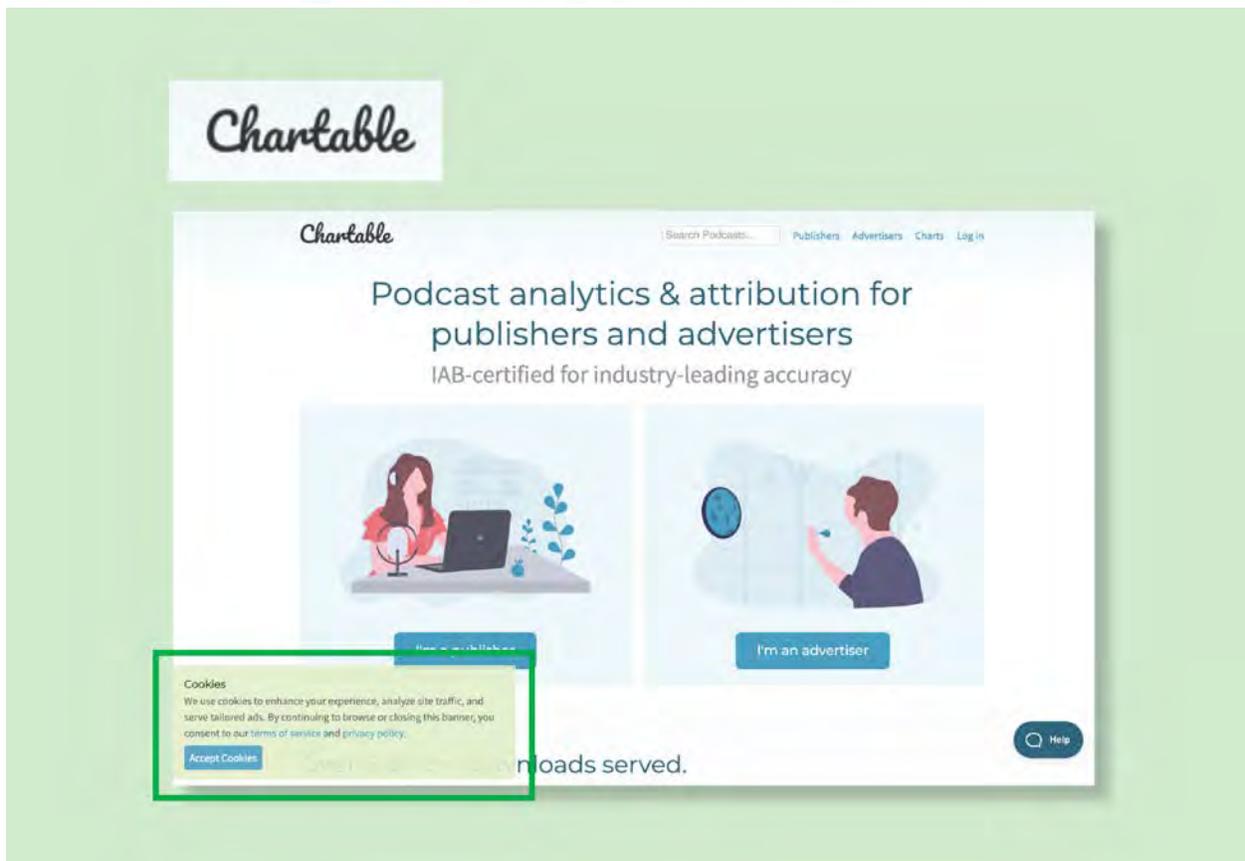
deleted without the consumer's consent, in the case of an opt out, it frustrates consumers' objectives to stop the sale of their personal information and does not provide additional privacy protection.

Some data brokers led consumers to abandon opt outs by forcing them to accept cookies.

As the CCPA went into effect in January 2020, some California consumers noticed that when they visited websites, they were asked to opt in to the use of cookies—and expressed confusion about what they were being asked to do. These notices have been common in Europe in response to the e-Privacy Directive, and more recently the Global Data Protection Regulation, though privacy advocates have been deeply critical of the practice: companies often use dubious dark patterns to nudge users to click “OK,” providing the veneer, but not the reality of, knowing consent.⁵⁶ The expansion of cookie banners in California was borne out in our study. Sixty-six of the 214 brokers had at least one consumer report a request or mandate to accept cookies as part of the DNS process. In some cases, for example if a company only tracks online using cookies, it may be reasonable for a site to set a non-unique opt-out cookie to allow the opt out to persist across multiple sessions. But the examples we saw were confusing to consumers, and did not clearly convey that a cookie was going to be placed for the limited purpose of enabling the opt out of cross-site data selling. And, as previously noted, sometimes the cookie consent banners obscured links to opt-out processes on a company's home page (see discussion of Freckle I.O.T./PlacelQ's interface, *supra* p. 21-22, and *infra* p. 31).

When visiting the website of the data broker Chartable to opt out of the sale of information, visitors are required to accept cookies. Chartable explains that the cookies are used to “serve tailored ads.” The only option is to “Accept Cookies,” and it asserts that by browsing the site users are agreeing to its terms of service and privacy policy.

⁵⁶ *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent*, PRIVACY INTERNATIONAL (last visited Aug. 28, 2020), <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>.



For nine brokers, at least one tester reported refraining from accepting cookies as part of the process. In five of these cases, testers reported that they stopped their request because they felt uncomfortable or did not understand next steps. For example, a Freckle I.O.T./PlacelQ tester described how accepting cookies was implicitly required for making a DNS request:

Their text-box asking to Allow Cookies covers the bottom 20% of the screen and won't go away unless, I assume, you tick the box to Allow. Therefore, I cannot see all my options. Also, I am accessing their site on a PC and they want me to download an app to my phone. Very difficult or impossible to see how to stop them from selling my data.

Another tester reported that the company they tested, Deloitte Consulting, had "two request types—'Cookie Based' and 'Non-Cookie Based'" and that they were "skeptical that most people will be able to decode the techno-babble description of each type."

Consumers were often forced to wade through confusing and intimidating disclosures to opt out.

While our survey did not include direct questions about communications with data brokers, in some cases consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, “There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart.” Another said of Oracle America, “The directions for opting out were in the middle of a wordy document written in small, tight font.” Another found the legal language used by Adrea Rubin Marketing intimidating: “they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury.”

Another data broker, ACBJ, placed a “Your California Privacy Rights” link at the bottom of their homepage (rather than a “Do Not Sell My Personal Information” link), which led to their privacy and cookie policy.⁵⁷ Once on the policy page, the consumer is forced to search in their browser for the phrase “Do Not Sell My Personal Information” or scroll and scan ten sections of the privacy policy to find the paragraph with a “Do Not Sell My Personal Information” link, or follow two additional links to navigate from the privacy policy table of contents to the “Do Not Sell My Personal Information” link. Upon clicking the “Do Not Sell My Personal Information” link, the consumer is shown a pop-up with a page of additional legal information, and then has to scroll down to a toggle that finally allows them to request their data not be sold.

Some consumers spent nearly an hour, if not more, to complete a request.

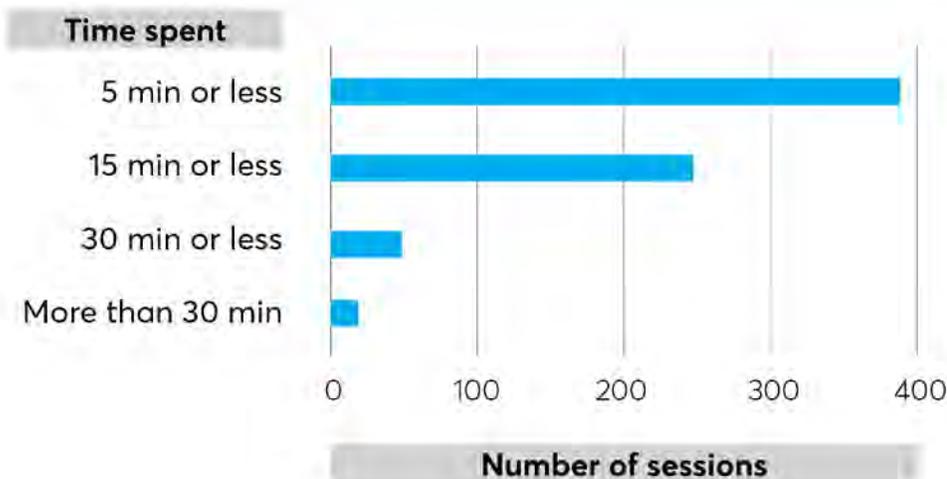
We also asked consumers about how long they spent to complete a request, and to not include the time spent filling out the survey. While the vast majority of consumers spent less than 15 minutes at a time on requests—and the most common amount of time was less than 5 minutes—some consumers reported that they nearly an hour or more than an hour opting out. A consumer working on the Jun Group reported that they were required to obtain their advertising ID to opt out: “Obtaining my Advertising Identifier was very time consuming and I am not sure how it is used.” The consumer testing Accuity reported: “They make it so hard to even find anything related to my information collected or subscribing or op-out that I had to read through so much boring yet infuriating do to what they collect and every one the will give it to for a price. We, as

⁵⁷ ACBJ (last visited Aug. 10, 2020), <https://acbj.com/privacy#X>.

Americans shouldn't have to do this to keep our information out of advertising collectors.”

Even spending five minutes on a single opt-out request could prevent consumers from exercising their CCPA rights. A consumer would have to make hundreds of such requests to be opted out of all data brokers potentially selling their data—not to mention all of the other companies with which the consumer has a relationship.

Sessions By Time Spent



At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.

Participants reported giving up in 7% of tests.⁵⁸ They reported being unable to proceed with their request in another 7% of tests.⁵⁹ These 14% of cases represent a DNS process clearly failing to support a consumer's CCPA rights.

⁵⁸ Example responses coded as “giving up” include: “Dead ended, as I am not going to send the info requested” and “Gave up because too frustrating. . .”

⁵⁹ Example responses coded as “unable to proceed” include “the website is currently waiting for me to provide my IDFA number but I'm not sure how to adjust my settings to allow the new app permissions to retrieve;” “I could not Submit my form after several tries;” and “It looks like I did not email them after

The overwhelming reason for a consumer to refrain from part of a DNS request process, or give up all together, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: "I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty." Even consumers that ended up providing the drivers' license ended up confused by the company's follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: "After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that '[w]e will update the ranges in the future release.' I have no idea what that means." Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.

The data broker X-Mode used data submitted as part of a DNS request to deliver a marketing email, a practice that is prohibited by the CCPA.

X-Mode, a data broker that sells location data, used customer data provided to opt out in order to send a marketing email, in violation of the CCPA. Study participants voiced concerns about handing over additional personal information to data brokers in order to protect their privacy, and it was disappointing to discover that their concerns were warranted. Consumers are particularly sensitive about receiving additional marketing messages. One consumer, for example, shared with us that they began receiving more unsolicited robocalls after submitting the opt-out request. Reflecting these concerns, the CCPA specifically prohibits companies from using data collected to honor an opt-out request for any other purpose.⁶⁰

getting nowhere calling the number on their website that was supposed to handle requests and had no idea what I was talking about."

⁶⁰ Cal. Civ. Code § 1798.135(a)(6).

But X-Mode ignored that requirement. X-Mode is a data broker that pays apps—such as weather and navigation apps—to collect location data from devices that have installed the software.⁶¹ X-Mode makes money by selling insights drawn from that data to advertisers. For example, the Chief Marketing Officer of X-Mode explained, “If I walked by a McDonald’s but walk into a Starbucks, my device knows with the XDK that I passed a McDonald’s but I actually went into Starbucks.”⁶² X-Mode also sells personal information to third party applications and websites.⁶³ And it has also shared anonymized location data with officials in order to help track compliance with stay-at-home orders during the COVID-19 crisis.⁶⁴ Because it sells such sensitive information, X-Mode should be particularly careful to protect the anonymity of consumer data and respect consumers’ privacy preferences.

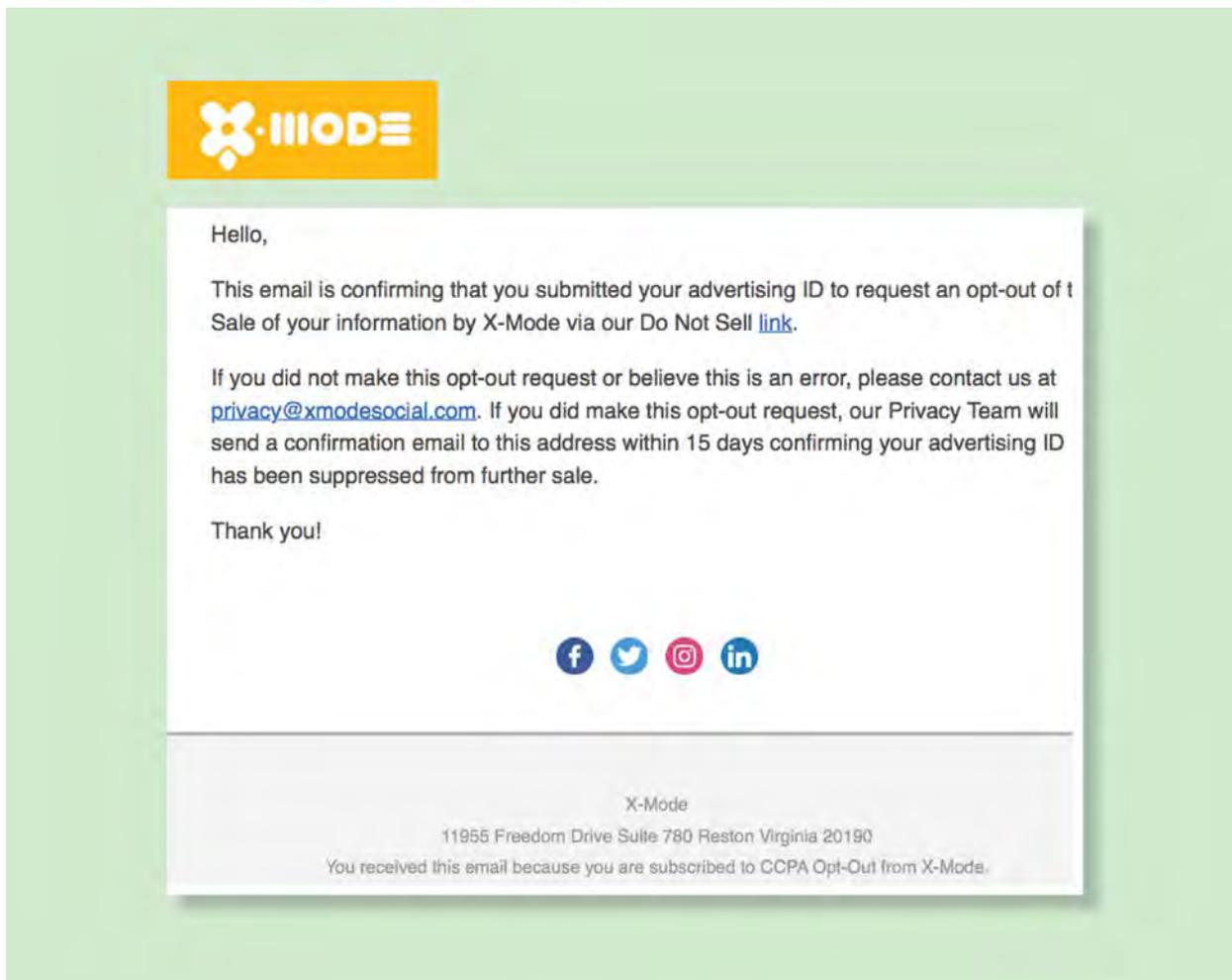
After submitting the opt-out request in April 2020, the author received the following email confirming that she had been placed on an “CCPA Opt-out” mailing list:

⁶¹ Sam Schechner et al., *Tech Firms Are Spying on You. In a Pandemic, Governments Say That’s OK*, WALL ST. J. (June 15, 2020), <https://www.wsj.com/articles/once-pariahs-location-tracking-firms-pitch-themselves-as-covid-sleuths-11592236894>.

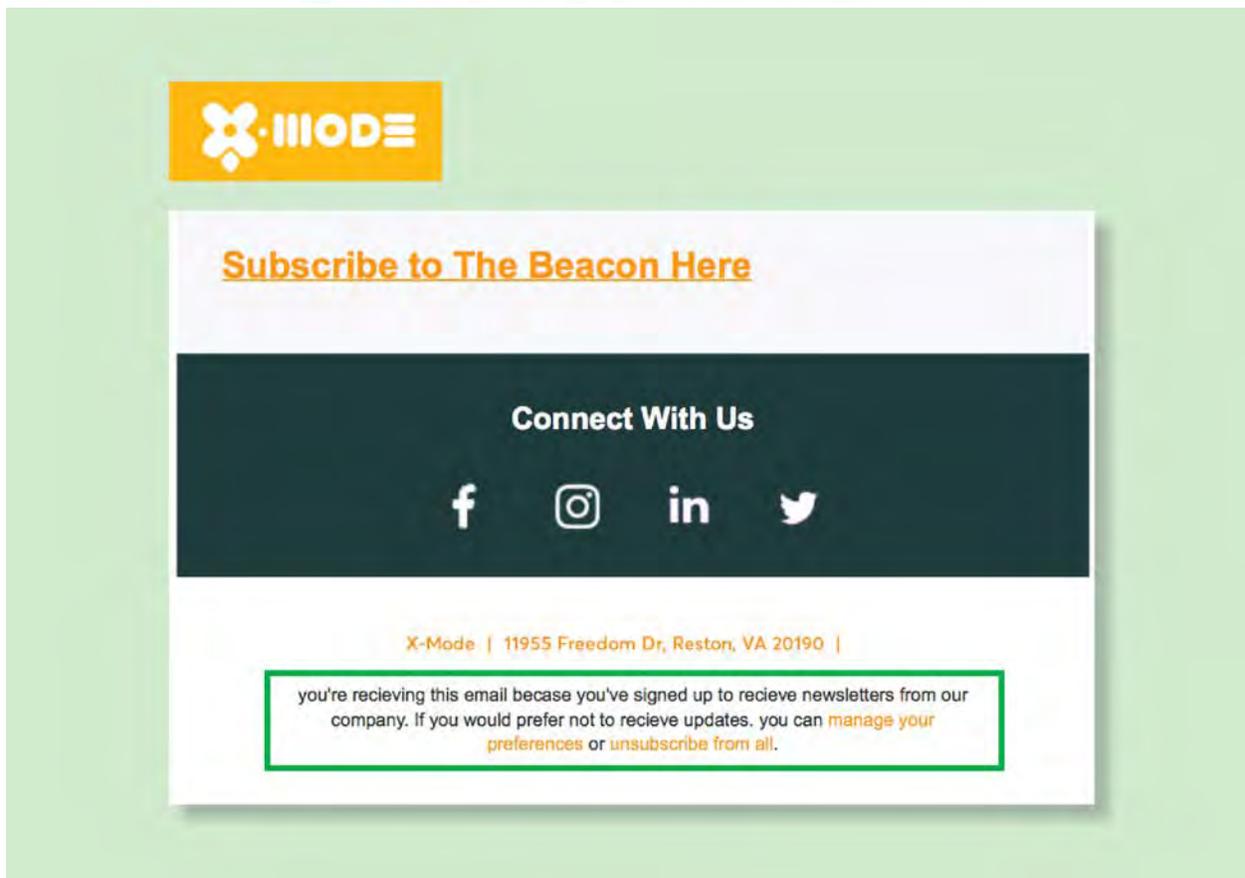
⁶² Jake Ellenburg, quoted in Karuga Koinange, *How Drunk Mode, An App for the Inebriated, Became Data Location Company X-Mode Social*, TECHNICALLY (Feb. 27, 2020), <https://technical.ly/dc/2020/02/27/how-drunk-mode-app-became-data-location-company-x-mode-social/>.

⁶³ ZenLabs LLC, Privacy Policy (last visited Aug. 28, 2020), <http://www.zenlabsfitness.com/privacy-policy/>.

⁶⁴ Schechner et al., *Tech Firms Are Spying on You*, *supra* note 61.



The following month, the author received an email inviting her to subscribe to X-Mode's newsletter in order to keep up with the business. The fine print explained that the email was sent "because you've signed up to receive newsletters from our company[,]" with the option to unsubscribe.

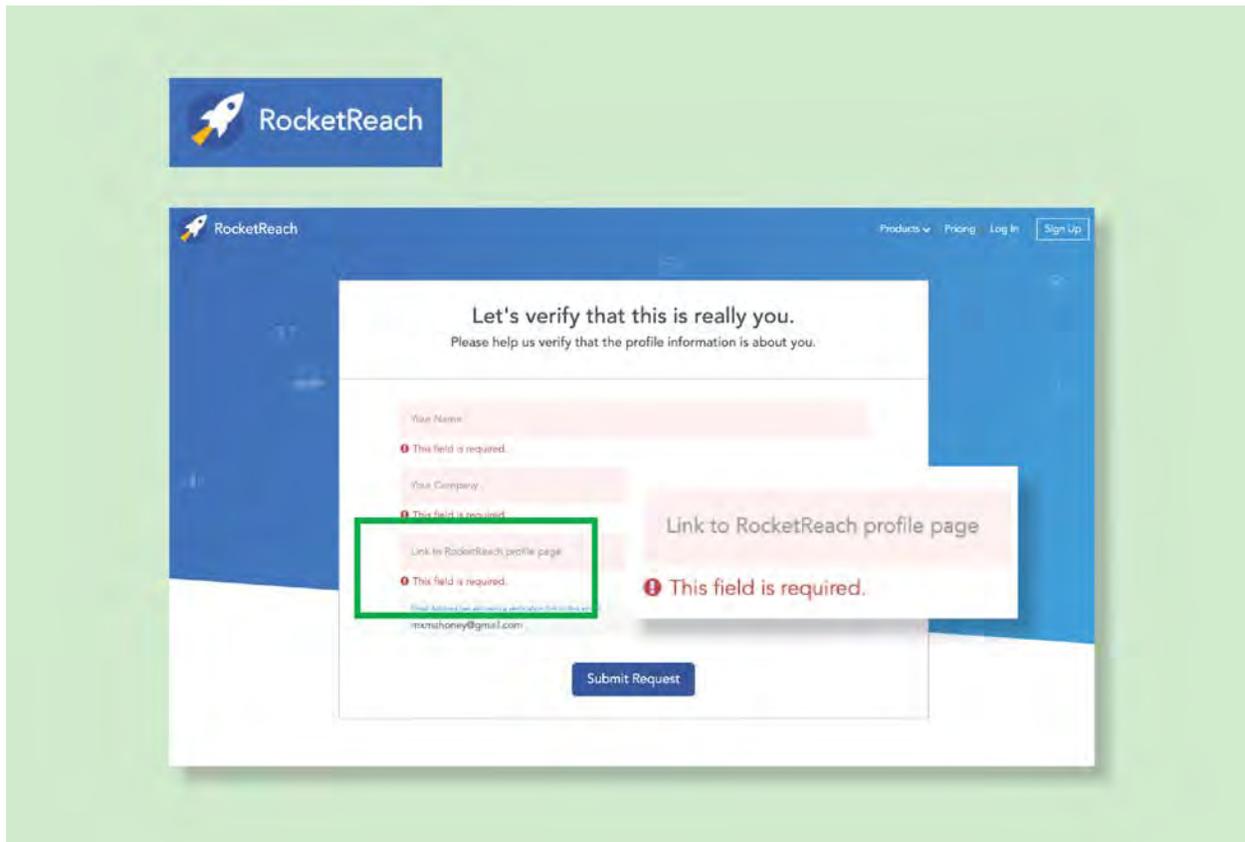


Since the only interaction that the author has had with X-Mode was to opt out—by definition, data brokers do not have relationships with consumers—the only way that she could have “signed up” was through opting out of the sale of her information. This behavior violates the CCPA’s prohibition on reuse of data provided for exercising data rights, and it could have a chilling effect on consumers exercising their rights with respect to other companies, as they are understandably worried about subjecting themselves to even more messages.

The data broker RocketReach requires the user to set up an account to opt out, which is prohibited by the CCPA.

RocketReach, a company that helps users find the contact information of potential business leads, requires users to list their RocketReach account in order to opt out of the sale of their information, even though the CCPA explicitly prohibits requiring

consumers to set up an account to opt out.⁶⁵ The homepage includes a link that reads “Do Not Sell My Info,” which then takes the consumer to a page that requires them to list their name, company, link to RocketReach profile, and email. If the user enters only name and email, the site does not let the user proceed further.



This frustrated testers, one of whom said, “I cannot determine whether they hold any of my information because they require a company and RocketReach account profile in order to honor the do not sell request.”

About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.

Neither the CCPA nor the implementing regulations require companies to notify consumers when their opt-out request has been honored, and this left consumers

⁶⁵ Cal. Civ. Code § 1798.135(a)(1).

confused about whether the company was still selling their information. Only in 18% of requests did participants report a clear confirmation from the broker that their data was or would soon not be sold. **In 46% of tests, participants were left waiting or unsure about the status of their DNS request.** In the 131 cases where the consumer was still waiting after one week, 82% were dissatisfied with the process (60% reported being very dissatisfied, and 22% reported being somewhat dissatisfied). The lack of clarity and closure was reflected in consumer comments such as “left me with no understanding of whether or not anything is going to happen” and “While it was an easy process—I will read their privacy policy to see if there is more [I] have to do to verify they are complying with my request. They left me unsure of the next step.”

In looking at how often consumers gave up or were unable to complete requests, we found a wide variety of responses from brokers, and variation in how consumers interpreted those responses. Once a DNS request was submitted, broker responses included:

- no response at all;
- acknowledging the request was received but providing no other information;
- acknowledging the request was received and vague language leaving consumers unsure of what was next;
- saying the request would be implemented in a certain timeframe (ranging from 2 weeks to 90 days);
- asking consumers to provide additional information;
- confirming a different type of request (such as Do Not Contact or Do Not Track);⁶⁶
- telling the consumer that the broker is not subject to the CCPA (even though the company was listed on the California data broker registry);
- telling the consumer that the broker has no data associated with them; and
- acknowledging the request was received and confirming that data will no longer be sold.

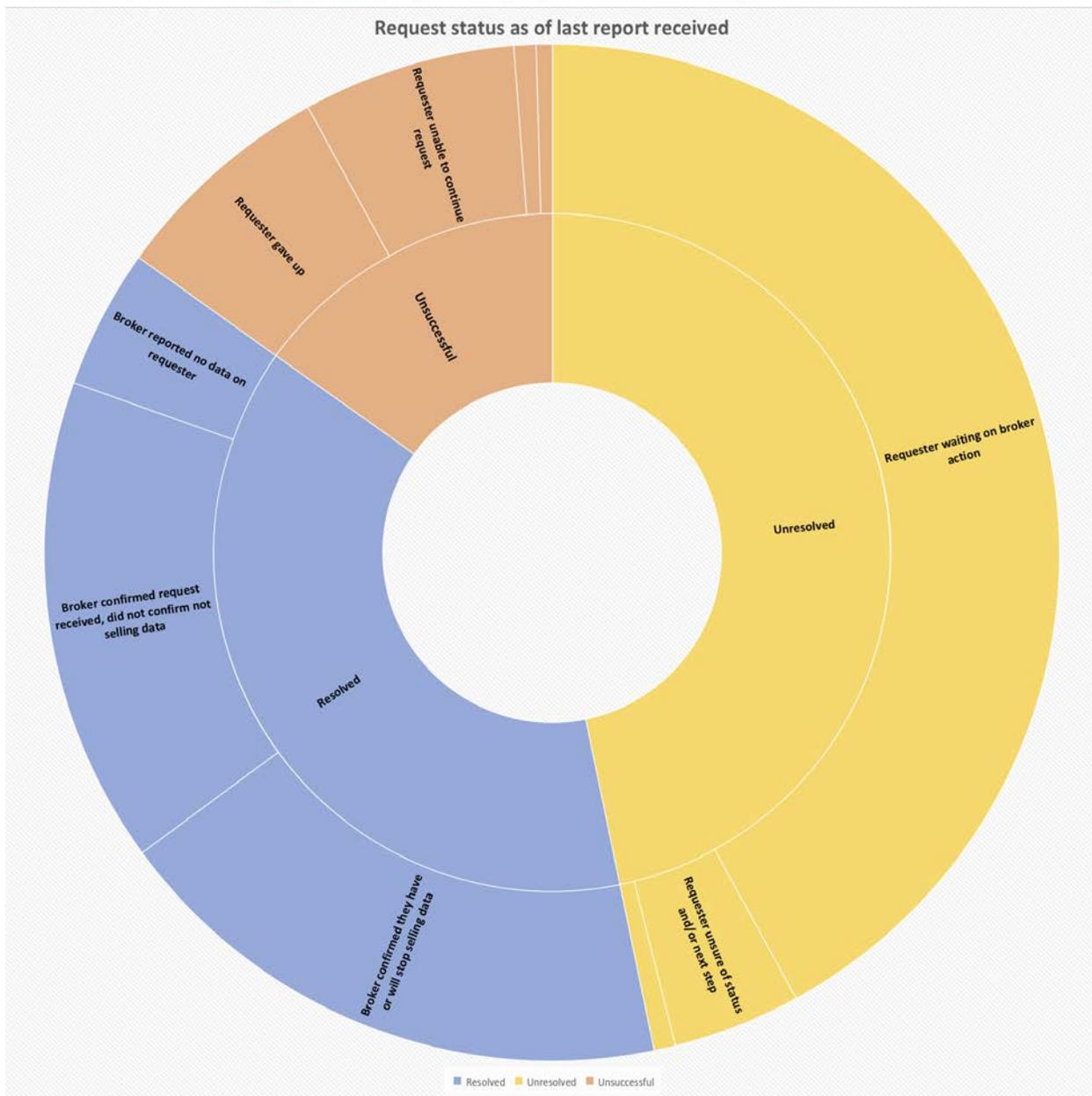
Consumers' understanding of these responses varied. For example, among participants reporting that the broker said that their request was received and that it would be

⁶⁶ Testers' references to “Do Not Contact” likely refer to consumers' right to be added to a company's internal “Do Not Call” list under the Telemarketing Sales Rule, 16 CFR § 310.4(b)(1)(iii)(A). Do Not Track refers to a request to stop tracking information about a consumer's activity across multiple sites. California law requires companies that collect personal information to disclose in the privacy policy whether they honor Do Not Track. See Cal. Bus. Prof. Code § 22575(5).

implemented in a certain time frame, some said the broker was honoring their DNS request but most said they were still waiting or unsure of the status of their request.

Below is a chart and visualization of the proportions of requests with different statuses as of the last report for each request:

Overall Status	Sub Status	Number Requests
Resolved	Broker confirmed they have or will soon stop selling data	107
	Broker confirmed request received, did not confirm not selling data	91
	Broker reported no data on requester	26
Unresolved	Requester waiting on broker action	247
	Requester unsure of status and/or next step	24
	Requester has outstanding follow up	4
Unsuccessful	Requester gave up	42
	Requester unable to continue request	40
	Broker reported not subject to CCPA	4
	Broker confirmed non-DNS request	3



We took a closer look at requests in which participants were “waiting” as of their last report, and found that many were still waiting for the data broker to respond to them after 21 days. Among the 247 requests in which the consumer was waiting for broker action, 81 were waiting after 21 days, 50 were waiting after at least a week but less than 21 days, and 116 of these were within 2 days of initiating a request. Those 116 represent cases where the broker may follow up later. However, the 81 cases in which consumers were still awaiting broker action after 21 days represent a problem with the

CCPA, in which consumers must choose between giving up and staying engaged for weeks at a time in hopes of receiving a clear confirmation from the broker that their DNS request has been completed. In 17 requests, the tester reported in an open-ended answer that they had had no response at all from the broker. Seven of these reports were after 21 days, and another 4 were after at least one week.

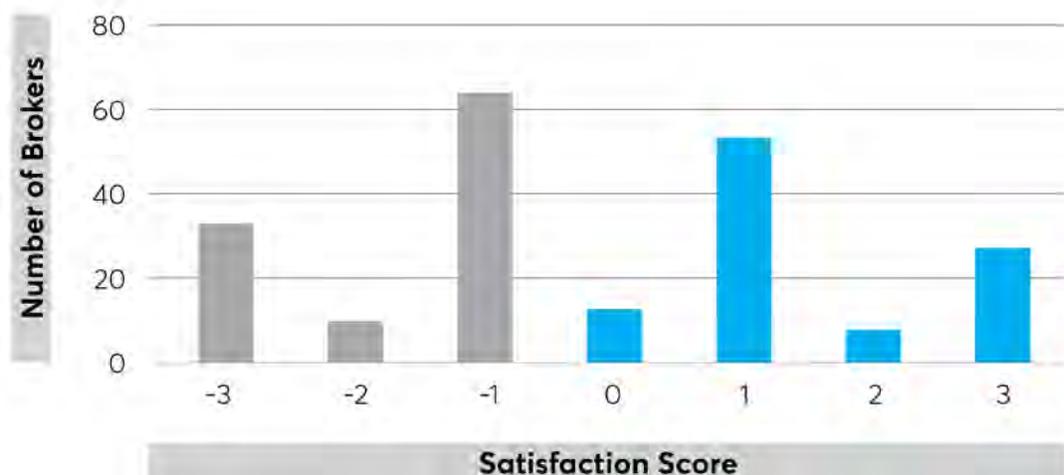
About 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with opt-out processes.

Overall, testers were more often dissatisfied than satisfied with the DNS processes. The survey asked how satisfied testers were with the process by providing four answers: very satisfied, somewhat satisfied, somewhat dissatisfied, very dissatisfied. The question was optional. Of the testers who answered this question, about 52% of the time, the tester was somewhat or very dissatisfied, and about 47% of the time, the tester was very or somewhat satisfied.⁶⁷

We also assigned each broker a satisfaction score. Some companies had consistent satisfaction, others had consistent dissatisfaction, and most had processes leaving consumers mixed in their satisfaction levels. In the satisfaction score, a broker received a positive point for a “very satisfied” or “somewhat satisfied” answer, and a negative point for a “somewhat dissatisfied” or “very dissatisfied” answer. The number of brokers with each score is plotted on the next page.

⁶⁷ Testers answered this question in 601 tests. Of these tests, in 317 (52%), the respondent was “somewhat dissatisfied” or “very dissatisfied” with the opt-out process, and in 284 (47%) tests, the respondent was “very satisfied” or “somewhat satisfied.” In 41 cases, the tester did not answer the question.

Tester Satisfaction



Some data brokers had quick and easy opt-out processes, showing that companies can make it easier for consumers to opt out. About 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

In several cases, consumers reported either a one-step process using an online interface that confirmed their data would no longer be sold, or a prompt and clear confirmation via email from the broker that their data would no longer be sold. For example, one tester of American City Business Journals described the process: “Just had to go to the privacy link at the bottom of the home page. Found the Calif. privacy link then had to scroll to button to turn off 'sell my info'.” Another shared an email from a DT Client Services, received the same day she submitted her request, that clearly confirmed that they would stop selling her data: “We confirm that we have processed your Request and will not sell your personal information to third parties.” These processes demonstrate an effective standard for implementing DNS requests. Overall, about 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

It is also possible for data brokers to post DNS links that are easy to find. For example, for 58% of the brokers, all three testers found the DNS link on the broker’s website, suggesting that these links were posted prominently. Links that were easy to find were

described as “prominent and easy to find,” “at bottom of page, but large,” “bottom of page, bold,” and “prominent at bottom of home page.” Thirty-nine data brokers out of 214 had all three testers report that the DNS link was “very easy” to find. For brokers where three out of three testers found the DNS link, the link was reported “very easy” or “somewhat easy” to find in 65% of cases, and “very difficult” or “somewhat difficult” to find in only 13% of cases.

Policy recommendations

The Attorney General should vigorously enforce the CCPA to address noncompliance.

The AG should use its enforcement authority to address instances of noncompliance, and to incentivize other companies to comply. While the AG is hamstrung by flaws in the enforcement provisions of the privacy requirements, notably the “right to cure” language that lets companies off the hook if they “cure” the problem within 30 days,⁶⁸ taking action will help push companies to get into compliance. Our study showed that a few improvements would go a long way. For example, it was significantly easier to opt out of a data broker site when the company had a link clearly labeled “Do Not Sell My Personal Information” that took consumers directly to the interactive form. Once that element was removed, consumers were often adrift, forced to email customer service staff who may not understand the request, or sent through a maze of sites with confusing disclosures. The AG should make an example of companies that fail to meet these requirements to help bring all of them into compliance.

To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales with a single step.

At the very least, consumers need access to universal opt-out tools, like browser privacy signals. Requiring consumers to opt out of every company one-by-one simply is not workable. The AG regulations require companies to honor platform-level privacy signals as universal opt outs, if the signal clearly constitutes a “Do Not Sell” command.⁶⁹ At the moment, however, there are no platform signals that we are aware of that clearly indicate a desire to out of the sale of data. Browsers are a logical place to start, though consumers need ways to opt out of advertising on devices other than browsers, such as

⁶⁸ Cal. Civ. Code § 1798.155(b).

⁶⁹ Cal. Code Regs. tit. 11 § 999 315(c) (2020).

TVs and phones. The AG should encourage developers to bring to market these solutions as quickly as possible, and should also set up a registry to help identify the signals that must be honored. This would help bring clarity for businesses and consumers.

The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.

Given that many consumers found it difficult to find the Do Not Sell link—it was often labeled with something different, and often buried at the bottom of the page with a bunch of other links—a graphic button would likely have value in ensuring that consumers would take advantage of that privacy protection. The CCPA directs the AG to design an opt-out button: “a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.”⁷⁰ The AG designed an initial draft, but declined to include a design in the final regulations. According to the AG, the proposed opt-out button was “deleted in response to the various comments received during the public comment period. The OAG has removed this subsection in order to further develop and evaluate a uniform opt-out logo or button for use by all businesses to promote consumer awareness of how to easily opt-out of the sale of personal information.”⁷¹ While the original design came under a fair amount of criticism, a uniform button, regardless of what it ends up looking like, will likely have value for consumers seeking to opt out, and the AG should promulgate one as soon as possible.

This will also help address instances in which companies route consumers through multiple, unnecessary steps in order to opt out. For example, Outbrain (*infra*, p. 18) led consumers through multiple steps to opt out, and on nearly every page the consumer had to hunt to figure out which option would lead them to the next step. And after all that, at least one consumer told us that they were not sure they had even opted out. Given that 7% of our testers gave up on the opt outs out of frustration or concern about sharing additional information, confusing interfaces significantly undermined consumers' ability to opt out.

⁷⁰ Cal. Civ. Code § 1798.185(a)(4)(C).

⁷¹ FSOR, *supra* note 27, at 15.

The AG should require companies to notify consumers when their opt-out request has been honored.

Many consumers had no idea whether or not their opt-out request had been honored. The uncertainty often left consumers dissatisfied with the opt out. Some companies did notify consumers that their requests had been honored, and this information was characteristic of simple, quick, and effective opt-out processes.

Required notification is also important for compliance purposes. For example, the AG regulations require companies to comply with opt outs within 15 business days. Without providing any notification of the opt out completion, there's no way to judge whether or not the company has honored the law and to hold them accountable if not.

The legislature or AG should clarify the definitions of “sale” and “service provider” to more clearly cover data broker information sharing.

In response to the CCPA, many companies have avoided reforming their data practices in response to “Do Not Sell” requests by arguing that data transfers either are not “sales,” or that transferees are “service providers” such that opt-out rights do not apply.⁷² Certainly, while some sharing with true data processors for limited purposes should not be subject to opt-out requests, many companies' interpretation of the CCPA seems to argue that third-party behavioral targeting practices are insulated from consumer choice.⁷³ As such, even if a consumer successfully navigates a DNS request from a data broker, in practice exercising opt-out rights may have little to no practical effect. Policymakers should close these potential loopholes to clarify that, *inter alia*, data broker information sharing for ad targeting is covered by CCPA obligations.

Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.

⁷² Mahoney, *Companies Aren't Taking the CCPA Seriously*, *supra* note 5.

⁷³ IAB CCPA Compliance Framework for Publishers & Technology Companies, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf; Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019), <https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175>.

While our study demonstrates that too many companies do not appear to be complying in good faith with the CCPA, any model that relies upon individuals to affirmatively act to safeguard their privacy will be deeply flawed. Given the challenges posed to businesses and consumers with respect to opting out, a better model is to ensure that privacy is protected without the consumer having to take any additional action. Several consumers who signed up for the study expressed shock that they were expected to opt out of the sale of their information. The thought of having to work their way through the entire data broker registry, which had hundreds of companies, was near unimaginable for these participants. Hard-to-find links, if they're even posted at all, confusing opt-out processes, requiring consumers to submit additional personal information, and above all the fact that there are hundreds of data brokers on the registry alone—all suggest that the responsibility needs to be on the company to protect privacy in the first place, rather than placing all the responsibility on the consumer.

This is a particularly important issue for elderly consumers or others who may have difficulty navigating online, several of whom dropped out of our study because it was so challenging to complete a single opt out. While there may be an easier path forward for some consumers who are able to take advantage of browser privacy signals to opt out universally—those are people who are already fairly tech savvy in the first place. Further, such a system only limits the sale of online data or data collected via a platform; it wouldn't stop the sale of data collected, say, in physical stores.

A better model would simply be to prohibit the sale of personal information as a matter of law, and to mandate that companies only collect, share, use, or retain data as is reasonably necessary to deliver the service a consumer has requested. Consumer Reports has supported legislation to amend the CCPA, AB 3119 (2020), that would require just that; Senator Sherrod Brown has introduced similar legislation, the Data Accountability and Transparency Act of 2020, at the federal level.⁷⁴ While the CCPA and the California data broker registry law are important milestones that improve transparency and individual agency, ultimately a more robust approach will be needed to truly protect Californians' privacy.

⁷⁴ The Data Accountability and Transparency Act of 2020, Discussion Draft, <https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf>.

Conclusion

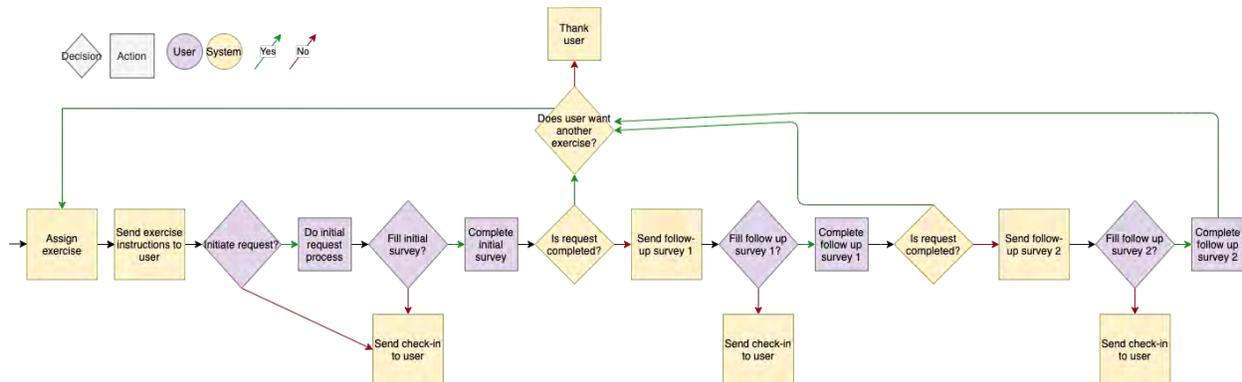
Overall, we found that consumers were too often dissatisfied with CCPA opt-out processes. This study uncovered some cases where the DNS process was short, clear, and satisfactory. It also found that some companies aren't complying with the CCPA, and that consumers were often left frustrated and without confidence that they had successfully exercised their DNS rights. It also reveals that, too often, consumers were unable to make a DNS request or gave up on the process altogether. Policymakers need to adopt crucial reforms in order to ensure that consumers can enjoy their right to privacy under the California Constitution.⁷⁵

⁷⁵ Cal. Cons. § 1.

Appendix

Section A

Below is a diagram of the participant experience of the exercise. Participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that broker. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker.



Section B

Below, we include links to screenshots of the homepages of data brokers that did not have the required “Do Not Sell My Personal Information” links on their homepages.*

[adMarketplace, Inc.](#)
[Big Brook Media, LLC](#)
[Blue Hill Marketing Solutions, Inc.](#)
[Comscore, Inc.](#)
[Electronic Voice Services, Inc.](#)
[Enformion, Inc.](#)
[Exponential Interactive, Inc. doing business as VDX.tv](#)
[Gale](#)
[GrayHair Software, LLC](#)
[Infinite Media Concepts Inc.](#)
[JZ Marketing, Inc.](#)
[LeadsMarket.com LLC](#)
[Lender Feed LC](#)
[On Hold-America, Inc. DBA KYC Data](#)
[Outbrain Inc.](#)
[PacificEast Research Inc.](#)
[Paynet, Inc.](#)
[PossibleNow Data Services, Inc](#)
[RealSource Inc.](#)
[Social Catfish LLC 1, Social Catfish LLC 2](#)
[Spectrum Mailing Lists](#)
[SRAX, Inc.](#)
[USADATA, Inc.](#)
[zeotap GmbH](#)

* On December 3, 2020, we replaced the screenshots for LeadsMarket, Social Catfish, and SRAX to provide a clearer view of the entire homepage.

Section C

An additional five companies had “Do Not Sell” links on their homepages, but all three testers were unable to find the DNS link, suggesting that it may not have been posted in a “clear and conspicuous manner” as required by the CCPA. Below, we include links to screenshots of the homepages of these companies.

[AcademixDirect, Inc.](#)

[Fifty Technology Ltd.](#)

[Freckle I.O.T. Ltd./PlacelQ](#)

[Marketing Information Specialists, Inc.](#)

[Media Source Solutions](#)

ADDENDUM TO UPDATED INFORMATIVE DIGEST

The OAG hereby incorporates this addendum to the updated informative digest as part of the final rulemaking package. As authorized by Government Code section 11346.9, subdivision (d), the OAG hereby incorporates the Informative Digest and the Updated Informative Digest prepared in this matter.

On November 3, 2020, Californians voted to approve Proposition 24, the California Privacy Rights Act (CPRA). While the CPRA substantially modifies the California Consumer Privacy Act (CCPA) and its implementing regulations, the majority of its provisions are not operative until January 1, 2023. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020) at § 31, subd. (a).) The small number of provisions that went into effect on December 16, 2020¹ do not impact any of the proposed modifications at issue in this rulemaking package. Moreover, the CPRA explicitly states that the CCPA shall remain in full force and effect and shall be enforceable until the CPRA becomes operative and enforceable. (*Id.* at subd. (c).)

The following provides a general description of the changes made to the regulations that went into effect on August 14, 2020.

Section 999.306 implements the CCPA by setting forth requirements regarding when and how a business must provide a notice of right to opt-out of sale to consumers, including requirements regarding the form, content, posting, and accessibility of the notice. (Civ. Code, § 1798.120, subd. (b); see also Civ. Code, §§ 1798.130, subd. (a)(2), 1798.135, subd. (a)(5).) The section has been modified to provide examples of how businesses that sell personal information that they have collected in the course of interacting with consumers offline can provide the notice of right to opt-out of the sale of personal information through an offline method.

Section 999.315 implements the CCPA by setting forth rules and procedures businesses must follow when a consumer requests that a business stop selling their personal information to third parties. (Civ. Code, §§ 1798.120, 1798.135.) The section has been modified to provide guidance on how a business's methods for submitting requests to opt-out should be easy and require minimal steps, including illustrative examples of prohibited methods because they are designed with the purpose or substantial effect of subverting or impairing a consumer's choice to opt-out. It has also been modified to provide a uniform icon required by the CCPA for the purpose of promoting consumer awareness of the opportunity to opt-out of the sale of personal information. (Civ. Code, § 1798.185, subd. (a)(4)(C).)

Section 999.326 implements the CCPA by setting forth rules and procedures regarding how businesses must handle requests made by an authorized agent of the consumer. (Civ. Code, §§ 1798.135, subd. (a)(1), 1798.135, subd. (c), 1798.140, subd. (y).) The section has been

¹ Cal. Const. art. II, § 10; Civ. Code, §§ 1798.145, subs. (m) and (n), 1798.160, 1798.185, 1798.199.10 through 1798.40, and 1798.199.95.

modified to clarify the proof that a business may require an authorized agent to provide, as well as what the business may require of a consumer to verify their request.

Section 999.332 implements the CCPA by setting forth the rules and procedures businesses must follow with regard to specific notices businesses shall include as it relates to minors under the age of 16 years old. This section has been modified to clarify that businesses subject to either section 999.330, section 999.331, or both of these sections are required to include a description of the processes set forth in those sections in their privacy policies.

Except as set forth above, there are no other substantial changes in applicable laws or to the effect of the proposed regulations apart from the laws and effects described in the Notice of Proposed Rulemaking Action.

SECOND ADDENDUM TO FINAL STATEMENT OF REASONS

BACKGROUND

The OAG hereby incorporates this second addendum as part of the final rulemaking package. As authorized by Government Code section 11346.9, subdivision (d), the OAG hereby incorporates the Initial Statement of Reasons (ISOR), the Final Statement of Reasons (FSOR), and the Addendum to the Final Statement of Reasons prepared in this matter.

All modifications in the fourth set of proposed modifications to the regulations are summarized below. All references to regulations are to Title 11 of the California Code of Regulations.

Changes Made to Article 2. Notices to Consumers

A. 11 CCR § 999.306. Notice of Right to Opt-Out of Sale of Personal Information.

Subsection (b)(3) further implements Civil Code section 1798.135, subdivision (a), regarding how to make the notice of right to opt-out reasonably accessible to consumers. The section contemplates scenarios in which businesses sell personal information collected from consumers in the course of interacting with them offline and require that the businesses use an offline method to inform the consumers of their right to opt-out and how to submit a request to opt-out. This subsection is necessary so that consumers interacting with businesses offline have the same information and opportunity to exercise their right to opt-out of the sale of their personal information as consumers who engage with businesses online. It also provides guidance to businesses on how to inform consumers in an offline manner through two examples. The subsection is narrowly tailored to only apply to businesses that are selling personal information that they collected from consumers in the course of interacting with them offline to avoid notice fatigue and confusion for the consumer.

Subsection (f) implements Civil Code section 1798.185, subdivision (a)(4)(C), for the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information. The OAG selected the blue toggle icon after testing a number of different graphics with consumers and finding that the blue toggle icon performed much better than the other graphics in communicating a consumer's choice over how websites can use their personal information. (See Cranor, et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* (February 4, 2020); Cranor, et al., *CCPA Opt-Out Icon Testing – Phase 2* (May 28, 2020).)

Throughout subsection (f), the word “button” from the originally proposed language has been replaced with “icon.” This is a non-substantive change that clarifies the text without materially altering the requirements, rights, responsibilities, conditions, or prescriptions contained in the original text. (Cal. Code Regs., tit. 2, § 40.) This change has been made for clarity and to align

the language to be consistent with the supporting studies that use the term “icon” instead of “button.” (See Cranor, et al., (February 4, 2020) and Cranor, et al., (May 28, 2020), *supra*.)

Subsections (f)(1) and (f)(2)’s requirement that the icon be used with, but not in lieu of, the “Do Not Sell My Personal Information” link is necessary because consumer testing has demonstrated that the icon alone does not communicate that consumers have choices regarding their personal information. (See generally, Cranor, et al. (February 4, 2020), *supra*.) At this time, there is not enough awareness or recognition of what the icon represents to replace every instance in which the “Do Not Sell My Personal Information” link is required under Civil Code section 1798.135, subdivision (a)(1). Businesses that seek to promote consumer awareness of the opportunity to opt-out of the sale of personal information may use the icon with the “Do Not Sell My Personal Information” link. **Subsection (f)(1)** also allows for businesses to use the opt-out icon in addition to the “Do Not Sell My Personal Information” link in order to facilitate multiple pathways for the consumer to exercise their right to opt-out. (See Habib, et al., “*It’s a scavenger hunt*”: *Usability of Websites’ Opt-Out and Data Deletion Choices*, CHI ’20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 2020, Honolulu, HI, USA, at pg. 7.) Thus, a business may use the icon graphic in addition to and outside the context of the “Do Not Sell My Personal Information” link on its homepage.

Subsection (f)(3) requires businesses to make the opt-out icon approximately the same size as other icons the business may use on its website (e.g., social media buttons or icons). This subsection is necessary to ensure that businesses make the icon as clear and conspicuous or otherwise accessible as other types of icons on a webpage. It also provides businesses with clear guidance about what is required of them.

Changes Made to Article 3. Business Practices for Handling Consumer Requests

B. 11 CCR § 999.315. Requests to Opt-Out.

Subsection (h) requires that a business’s methods for submitting requests to opt-out shall be easy for consumers to execute, shall require minimal steps, and shall not be designed with the purpose or with the substantial effect of subverting or impairing a consumer’s choice to opt-out. The subsection directly prohibits the use of dark patterns that undermine a consumer’s choice and are counter to the intent of the CCPA, which provides for a consumer’s robust right to request a business to stop selling their personal information. This regulation was made in response to comments raised earlier in the rulemaking process urging the OAG to address the issue of businesses using dark patterns to subvert a consumer’s choice to opt-out, the OAG’s experience enforcing the CCPA, and recent studies on consumers’ experience exercising their privacy choices. (See Paternoster, *Getting round GDPR with dark patterns. A case study: Techradar* (Aug. 12, 2018) <<https://www.leonpaternoster.com/posts/techradar-gdpr/>> [as of May 21, 2020]; Habib, et al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019, August 11-13, 2019, Santa Clara, CA, USA; Habib, “*It’s a scavenger hunt*,” *supra*; Luguri, Jamie and Strahilevitz, Lior, *Shining a Light on Dark Patterns* (August 1, 2019), University of Chicago, Public Law Working Paper No. 719, University of Chicago Coase-Sandor Institute for Law & Economics

Research Paper No. 879; Mahoney, et al., *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* (October 1, 2020), Consumer Reports.) As documented by the Consumer Reports study and the Habib study on the usability of websites, there is already abuse by businesses in this area, which these regulations intend to address. (See Mahoney, *supra*, pp. 4-5, 24-26; Habib, “*It’s a scavenger hunt,*” *supra*, pp. 7-9; Habib, *An Empirical Analysis, supra*, pp. 6-12.)

Subsections (h)(1) through (h)(5) provide specific examples that illustrate what is meant by this requirement. **Subsection (h)(1)** specifically prohibits businesses from requiring a consumer to go through more steps in opting out of the sale of personal information than the number of steps required for the consumer to opt-in to the sale of personal information after previously opting out. Instead of imposing a prescriptive standard based on the number of steps used, the regulation holds the business to a standard that the business would create for itself, *i.e.*, the flow process for opting into the sale of data. Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios, but also measurable and clearly enforceable. It addresses a common dark pattern that researchers characterize as a “roach motel” (easy to get in but hard to get out) and provides a concrete way for businesses to measure whether they are using a minimal number of steps. (See Luguri and Strahilevitz, *supra*, p. 7.) **Subsection (h)(1)** also identifies for businesses how to measure the start of the flow process for both the opt-out and opt-in process so that they can accurately compare the number of steps for both processes. Because the CCPA does not require that businesses obtain opt-in consent for the sale of personal information, except for consumers under the age of 16, the phrase “opt-in to the sale of personal information after having previously opted out” is used to advise businesses that the comparison of the opt-out process should be with the opt-in process for consumers 16 years and older.

Subsection (h)(2) prohibits a business from using confusing language, such as double-negatives, when providing consumers the choice to opt-out. The example of “Don’t Not Sell My Personal Information” is given as a clear example to businesses regarding what would be considered confusing language. This regulation addresses dark patterns posed as a “trick question” and generally confusing language that can have the substantial effect of subverting or impairing a consumer’s choice. (See Luguri and Strahilevitz, *supra*, p. 7; Habib, *An Empirical Analysis, supra*, p. 10; Habib, “*It’s a scavenger hunt,*” *supra*, pp. 6-8.)

Subsection (h)(3) prohibits a business from requiring consumers to click through or listen to reasons why they should not submit a request to opt-out, except as permitted by the regulations. This subsection is necessary because the OAG has seen abuse by businesses in this area. Dark patterns researchers refer to this practice as “confirmshaming.” (See Luguri and Strahilevitz, *supra*, pp. 6.) The regulation does, however, allow businesses to provide notice to consumers about partial opt-out options and other information about their right to opt-out through the inclusion of the phrase “[e]xcept as permitted by these regulations.” (See §§ 999.306, 999.315(d).) It also does not prohibit businesses from including information about why the

consumer should not opt-out elsewhere or through a link that consumers may click on. It narrowly prohibits businesses from requiring consumers to click through or listen to such reasons *during* the process of opting out, which would be an example of a method that subverts the consumer's choice.

Subsection (h)(4) prohibits a business from requiring consumers to provide personal information that is not necessary to implement the request, especially given that requests to opt-out need not be verified. Seeking additional personal information may deter or encumber consumers seeking to exercise their right to opt-out. (See Mahoney, *supra*, pp. 26-30, 33-34.) The regulation applies the internationally recognized fair information practice principle ("FIPP") of data minimization, *i.e.*, to only collect data directly relevant and necessary to accomplish the specified purpose. It does not impose a prescriptive restriction on required data points, but rather, places a performance-based standard on businesses to only require personal information that is necessary to implement the request. If a business cannot explain why the personal information is necessary, it should not require it from consumers. This regulation is necessary because the OAG has seen and consumer studies have documented significant abuse by businesses in this area. (*Ibid.*)

Subsection (h)(5) requires that the "Do Not Sell My Personal Information" link take the consumer directly to the mechanism for submitting a request to opt-out. It reaffirms the requirements set forth in section 999.306, subsections (b) and (c), and clarifies that any misdirection of the consumer would be considered a dark pattern that has the substantial effect of subverting or impairing the consumer's choice to opt-out. This regulation is necessary because the OAG has seen and consumer studies have documented significant abuse by businesses in this area. (See Mahoney, *supra*, pp. 32-33; Habib, *An Empirical Analysis, supra*, p. 12.)

Changes Made to Article 4. Verification of Requests

C. 11 CCR § 999.326. Authorized Agent.

Subsection (a) has been revised to clarify what a business may require of an authorized agent and the consumer when an agent makes a CCPA request on the consumer's behalf. This change is necessary because the regulation previously did not specify if the business can ask the authorized agent for proof of the consumer's signed permission. It only stated that the consumer provide signed permission to the agent. Also, as previously written, the regulation allowed the business to require the consumer to both verify their own identity directly with the business and directly confirm with the business that they provided the agent permission to submit the request. Requiring the consumer to do both would unnecessarily burden consumers' ability to use an authorized agent, which is contrary to the intent of the CCPA as set forth in Civil Code, sections 1798.135, subdivision (a)(1) and 1798.185, subdivision (a)(7).

Changes Made to Article 5. Special Rules Regarding Consumers Under 16 Years of Age

D. 11 CCR § 999.332. Notices to Consumer Under 16 Years of Age.

Subsection (a) has been revised to state that a business subject to sections 999.330 “and/or” 999.331 shall include a description of the processes set forth in those sections in its privacy policy. This change is necessary because, as previously written, the regulation could have been interpreted to apply to businesses that sell the personal information of both groups of minors—those under 13 years of age and those 13 to 15 years of age. This revision clarifies that the rules apply to a business that sells the personal information of one or both groups of minors and mandates that these businesses would be required to include a description of the process set forth in section 999.331 within its privacy policy.

SUMMARY OF COMMENTS AND DEPARTMENT RESPONSES

The OAG received 20 comment letters during the third 15-day comment period and 16 comment letters during the fourth 15-day comment period. The summary of the comments and the OAG’s responses to them are attached as the following appendices.

Appendix G. Summary and Response to Comments Submitted during 3rd 15-Day Period

Appendix H. List of Commenters from 3rd 15-Day Period

Appendix I. Summary and Response to Comments Submitted during 4th 15-Day Period

Appendix J. List of Commenters from 4th 15-Day Period

For ease of reference, the OAG assigned a number to each written comment received. The written comments for the third 15-day comment period begin with W377 because they follow consecutively after the comments submitted in the previous comment periods. The written comments for the fourth 15-day comment period begin with W397 for the same reason. Because most comment letters contained multiple substantive comments that needed to be addressed, for each substantive comment, the OAG assigned subnumbers to the comment number. For example, in the OAG’s summary and response to comments, the comment number “W377-3” refers to the third substantive comment included in the 377th written comment letter received.

Appendices G and I are organized according to the chronological order of the modified regulations that they address. Comments generally about the modifications, but not regarding a particular section or subsection of the regulations, are grouped together under the heading “General Comment Regarding All Modifications.” Page numbers have been included for ease of reference.

Appendices H and J identify the person and/or entity that submitted the comment during a particular comment period and provides the response number(s) that correspond(s) to the commenter’s substantive point(s). It is essentially an index that assists the commenter in locating the OAG’s response to their comment, given the extensive number of substantive

comments received. In some instances, the commenter's substantive point may have been responded to by more than one response number.

ALTERNATIVES DETERMINATIONS

In accordance with Government Code section 11346.9, subdivision (a)(4), the OAG has determined that no reasonable alternative it considered or that has otherwise been identified and brought to its attention would be more effective in carrying out the purpose for which the action is proposed, or would be as effective and less burdensome to affected private persons than the proposed action, or would be more cost-effective to affected private persons than the proposed action, or would be more cost-effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.

The alternatives considered and rejected are below. In considering the following alternatives, the OAG sought to balance the benefits to consumers, the burden to businesses, and the purposes of the CCPA.

Section 999.306, subd. (b)(3):

The OAG considered and rejected the alternative of including additional examples of how businesses can give notice of right to opt-out offline. This alternative is not as effective and less burdensome to affected private persons than the proposed regulation. Given the wide variety of different industries subject to the CCPA, there are many different ways in which to provide offline notice. The OAG has provided a few examples for clarification purposes, but businesses have flexibility to inform consumers in different ways. The adequacy of a notice of right to opt-out is a fact-specific analysis and prescribing additional examples may be too limiting.

Section 999.306, subd. (f):

The OAG considered and rejected the alternative of allowing the marketplace to determine the best opt-out icon design. This approach is not as effective and less burdensome to affected persons than the adopted regulation. Civil Code § 1798.185(a)(4)(C) requires the OAG to develop a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information. The OAG selected the blue toggle design after studying and testing a number of different graphics with consumers, including the DAA AdChoices icon. (See Cranor, et al., (Feb. 4, 2020), *supra*, at p. 3.) Those studies demonstrated that the blue toggle design performed much better than the other graphics in communicating a consumer's choice over how websites can use their personal information. (See Cranor, et al., (February 4, 2020) and Cranor, et al., (May 28, 2020), *supra*.)

Section 999.315, subd. (h)(1):

The OAG considered and rejected the alternative to replace the limitation on the number of steps a business may use in its opt-out process with the requirement that the business simply consider the number of steps an opt-out process takes as a factor in determining whether the process is

easy to use. The alternative is not as effective in carrying out the purpose and intent of the CCPA. As documented by the Consumer Reports study, businesses are using dark patterns to subvert the consumer's choice to opt-out. (See Mahoney, *supra*, pp. 4-5, 24-26.) Clear guidance with a measurable standard is necessary to curb this abuse. The regulation holds the business to a standard the business would create for itself, *i.e.*, the flow process for opting into the sale of data. Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios. The alternative would not be as effective in curbing abuse because it does not provide businesses with enough guidance regarding how to comply and would make the regulation harder to enforce.

Section 999.326, subd. (a):

The OAG considered and rejected the alternative to only allow businesses to require the consumer to directly verify their own identity when the authorized agent has not provided reasonable proof that the authorized agent has previously verified the consumer's identity. The alternative is not more effective in carrying out the purpose and intent of the CCPA. In drafting the regulation, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer's statutory right to use an authorized agent as required by the law. The OAG determined that giving businesses the discretion to require consumers to verify their identity directly with the business or directly confirm that they provided the authorized agent with their permission to submit their request is more effective in carrying out the purpose and intent of the CCPA than the alternative because it balances consumers' ability to exercise their rights while preventing fraud and abuse. Disclosing personal information, especially sensitive personal information, into the wrong hands may cause grave harm to consumers in certain circumstances. Businesses should have discretion to determine whether additional verification requirements are warranted based on the factors set forth in §§ 999.323(b), 999.324, and 999.325 of these regulations.

NON-DUPLICATION

Some of the regulations may repeat or rephrase in whole or in part a state or federal statute or regulation. This was necessary to satisfy the clarity standard set forth in Government Code section 11349.1, subdivision (a)(3).

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information				
- § 999.306(b)(3)				
1.	Opt-out notices in an offline setting should only be required if information collected in that offline setting or from an offline transaction is sold. For businesses that do not sell data collected offline, an offline notice will create consumer confusion by implying to consumers that the business does sell data collected offline. It would also be redundant and burdensome to businesses to require an offline notice when they do not sell data collected offline.	Accept. The OAG has revised the regulation to clarify that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of the sale of their personal information and how to submit a request to opt-out.	W383-1 W386-2 W387-1 W390-1 W393-1 W395-2	00083 00098-00099 00105-00107 00127 00149-00150 00160-00161
2.	Revise section 999.306(b)(3)(a) to give businesses the option of directing consumers to where the notice can be found online, such as through a web address or a QR code, consistent with section 999.305(b)(3) and proposed section 306(b)(3)(b). QR code technology is an efficient and practical means of providing information to consumers in offline environments and can add interactivity between businesses and consumers even in offline settings and can facilitate consumers’ exercise of privacy choices.	No change has been made in response to this comment. The OAG has revised the regulation to clarify that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of the sale of their personal information and how to submit a request to opt-out. In addition, the comment’s proposed change is unnecessary because directing consumers to where the notice can be found online is not prohibited by the regulation and the current language provides businesses with flexibility that includes posting a web address or QR code. The example provided in subsection (b)(3)(a) specifically states that a business may inform consumers by posting signage that directs consumers to where information can be found online. Businesses have the flexibility to deliver the notice in different ways provided that they are facilitating consumers’ awareness of their right to opt-out. Whether directing consumers to where information can be found online is sufficient to properly inform consumers of their right to opt-out is a fact-specific analysis for the business to undertake.	W384-1 W385-1 W395-4	00086-00089 00091-00092 00160-00161
3.	Include as illustrative examples that businesses can give notice “by the store entrance,” and when personal information is collected outside the store, such as in the parking lot, notice can be posted “in	No change has been made in response to this comment. This regulation provides guidance on how to make information about consumers’ right to opt-out reasonably accessible to consumers who interact with businesses offline so that they have the same	W386-3 W395-3	00099 00160-00161

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	<p>an area that is reasonably visible to consumers.” Requirement that signage be posted where personal information is collected could be read as prohibiting signage in more effective and noticeable locations, and because cash registers and point-of-sale locations are often high-interaction areas where consumers are unlikely to see the notices.</p>	<p>opportunity to exercise their right to opt-out as consumers interacting with the business online. The examples illustrate some ways in which a business may inform consumers by an offline method and consider as a factor when and how the consumer is providing their personal information. The examples are not exclusive. Businesses have the flexibility to inform consumers in different ways provided that they are facilitating consumers’ awareness of their right to opt-out. Whether to inform consumers by posting signs at the store entrance or in the parking lot is a fact-specific analysis for the business to undertake.</p>		
4.	<p>Revise to clarify that the notice should include what information is collected and sold and an explanation of how to opt-out of sales after the call is over. The notice of right to opt-out assumes the business already has some data about the consumers. Also, consumers may not be comfortable opting-out during the call.</p>	<p>No change has been made in response to this comment. The OAG disagrees with the comment’s assumption that the notice to opt-out assumes that the business already has data about the consumers. Section 999.305(b)(3) requires that the notice to opt-out be included with the notice at collection, which must be given at or before the point of collection of personal information. See also 2nd Addendum to FSOR, p. 1.</p>	W389-2	00123
5.	<p>Providing opt-out notices often depends on the actual circumstances when the data is collected. With regard to subsection (a), the opt-out notice could be provided at the point of entry into a business, at the time a consumer has to sign a waiver or make payment, and after visiting the facility if the business has the consumer’s contact information. The Attorney General may consider what possible steps would facilitate the creation of privacy icons displaying a business’s data-collection and data-use practices and how to ascertain that average consumers easily understand those data disclosures.</p>	<p>No change has been made in response to this comment, which is interpreted to be an observation rather than a specific recommendation to change these regulations. To the extent that the comment is suggesting that the OAG include additional examples of how to provide the notice offline, see response #3. Regarding a privacy icon, as authorized by Civil Code, § 1798.185, subd. (a)(4)(C), the OAG has revised the regulations to add an online uniform opt-out icon that businesses may use with the “Do Not Sell My Personal Information” link. See proposed § 999.306(f).</p>	W389-1	00121-00123
6.	<p>Strike section 306(b)(3)(a) and, in section 306(b)(3)(b), allow businesses communicating with consumers by phone to direct them to an online notice to satisfy the business’s offline notice</p>	<p>No change has been made in response to this comment. The OAG has revised the regulation to clarify that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of</p>	W388-5	00116-00117

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	<p>obligation rather than requiring businesses to read their full notice aloud over the phone. The proposed regulations are redundant and unnecessary, overly restrictive and prescriptive, would overwhelm consumers and cause privacy-notice fatigue, would restrict businesses' speech, would cause consumer confusion, and would remove the flexibility businesses need to communicate information to consumers in way that does not impede businesses' interactions with consumers.</p>	<p>the sale of their personal information and how to submit a request to opt-out. The OAG does not agree that providing these illustrative examples are overly prescriptive or unnecessary. This regulation provides guidance on how to make information about a consumer's right to opt-out reasonably accessible to consumers who interact with businesses offline so that they have the same opportunity to exercise their right to opt-out as consumers interacting with the business online. The examples illustrate some ways in which a business may inform consumers by an offline method and consider as a factor when and how the consumer is providing their personal information. The examples are neither exclusive nor exhaustive. Businesses have the flexibility to inform consumers in different ways provided that they are facilitating consumers' awareness of their right to opt-out.</p> <p>The comment also misconstrues the requirement that businesses must read the full notice aloud over the phone. The modification clarifies that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of the sale of their personal information and how to submit a request to opt-out. The OAG does not agree that directing the consumer to an online notice is sufficient; to avoid consumer confusion, businesses may need to also provide context for the notice, i.e., that it pertains to the consumer's right to opt-out of the sale of personal information and how to do it. The regulation does not prohibit directing the consumer to a webpage for more information provided that the business gives the consumer the appropriate context for what the webpage is about, i.e., that they have a right to opt-out and that they can do so through the webpage.</p>		
§ 999.315. Requests to Opt-Out				
- § 999.315(h) generally				
7.	<p>Supports the proposed regulation, which would protect against businesses using "dark patterns" to encumber consumers' exercise of their CCPA opt-</p>	<p>The OAG appreciates this comment of support. No change has been made in response to this comment. The comment concurred with the proposed regulations, so no further response is required.</p>	<p>W378-1 W382-1 W396-1</p>	<p>00005 00020-00024 00166</p>

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	out right. A Consumer Reports study shows that many consumers encounter challenges to opting out, and the regulations will address many of these issues.			
8.	The Attorney General should follow the emerging CCPA-compliance practices and regularly update the prohibited practices that hinder opt-outs in order to ensure that consumer protections remain meaningful. Because businesses tend to require consumers to provide additional information for verification purposes, leading to a cumbersome, time-consuming verification process for consumers, the Attorney General should provide non-binding guidelines and recommendations to help businesses transition to more efficient data practices.	No change has been made in response to this comment. The comment does not relate to any modification to the text for this 15-day comment period and is interpreted to be a general observation rather than a specific recommendation to change these regulations.	W389-3	00123-00124
9.	The Attorney General should promulgate the design for a uniform opt-out button, which will help consumers seeking to opt-out. One comment suggests using a previously submitted design for a Nutrition Label framework as a readily adaptable standard and functional implementation of an opt-out button.	Accept in part. The OAG has revised the regulation to add a uniform opt-out icon that businesses may use with the “Do Not Sell My Personal Information” link. See proposed § 999.306(f). The OAG did not implement a Nutrition Label framework because it implicates more than just the right to opt-out. Civil Code, § 1798.185(a)(4)(C) requires the OAG to develop a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information, as opposed to any privacy purpose. Moreover, in drafting these regulations, the OAG has considered the wide variety of different industries subject to the CCPA, as well as the costs to be incurred by the various businesses in complying with the law. For the reasons set forth in the ISOR, FSOR, and the second addendum to the FSOR, the OAG determined that the current framework implements the CCPA in a manner that provides flexibility and is cost effective and less burdensome on businesses. The comment’s proposed change to implement a mandatory Nutrition Label framework may not best address all the different factual situations and industries in which the	W382-2 W384-2 W394-2	00024 00089 00154-00155

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		CCPA requires disclosures at this time. However, the OAG appreciates the comment and continues to observe business trends and best practices as part of its ongoing rulemaking authority. Businesses should also consider best practices and the regulations do not prohibit privacy disclosures that benefit consumer understanding, such as the Nutrition Label framework.		
10.	The proposed regulation should be revised to require businesses to consider certain factors when creating opt-out processes, similar to the format of section 999.323(b)(3), rather than the current format of “illustrative examples” that are framed in a statutory “shall not” form that implies that businesses must comply with their prescriptions.	No change has been made in response to this comment. The comment’s proposed change is not more effective in carrying out the purpose and intent of the CCPA. This regulation was made in response to comments raised during the rulemaking process, as well as the OAG’s experience enforcing the law, where businesses are using methods that are designed to, or have the substantial effect of subverting or impairing a consumer’s choice to opt-out. Giving businesses discretion to comply with the five illustrative examples would not be as effective in curbing the use of such practices and would also be less effective in giving businesses clear direction on how to comply with the law.	W391-2	00130-00132
11.	Additional measures should be taken to ensure that businesses don’t subvert consumers’ ability to exercise their CCPA rights. Empirical research has shown a wide discrepancy in how businesses have implemented the opt-out process and evidence of “dark patterns” that impose unfair barriers to completing opt-out requests and that have disproportionate impacts on the elderly, non-English speakers, individuals with lower written literacy and technology experience, and other vulnerable individuals. Businesses should be required to: (1) Provide forms, rather than email addresses, for opt-out requests. Opt-out processes that require consumers to send an email, without identifying what information must be included, are burdensome on consumers.	No change has been made in response to this comment. At this time, the OAG does not believe that the comment’s proposals are necessary because current and proposed regulations address these concerns. See Section 999.315(a) (businesses required to provide an interactive form for submitting requests to opt-out); § 999.306(a)(2) (requires notice to opt-out be easy to read and understandable to consumers, and provided in languages in which the business in its ordinary course provides information to consumers); proposed regulation 999.315(h)(3) and (h)(5) (requires businesses to limit extraneous information from the process for submitting requests to opt-out). However, the OAG appreciates the comment’s suggestions and will continue to analyze whether additional regulations are necessary to address “dark patterns” as part of its ongoing rulemaking authority.	W392-1 W392-2 W392-3 W392-4 W392-5	00135-00136, 00139-00146 00136 00136, 00143 00137 00137

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	<p>(2) Offer opt-out forms in different languages and use simple, easy to understand language if they provide essential services or have a substantial non-English-speaking customer base.</p> <p>(3) Be prohibited from crowding opt-out forms with extraneous information. While providing references to useful information about the CCPA may be helpful, reproducing hundreds of words of text not required for opt-outs is not helpful and discourages consumers from completing opt-out requests.</p> <p>(4) Provide consumers a streamlined form that does not require them to take extraneous steps to complete an opt-out request, and to make the selection choices in multiple-purpose forms simple and clear.</p>			
12.	<p>Add a requirement that opt-out preferences must persist for at least as long as opt-in preferences. For example, if a consumer is able to opt-in indefinitely without further contact, then the business must not present daily opt-out dialogs.</p>	<p>No change has been made in response to this comment. The comment’s proposed change is unnecessary. Civil Code § 1798.135(a)(5) already requires the business to respect the consumer’s decision to opt-out indefinitely, and prohibits the business from asking the consumer to authorize the sale of their personal information for at least 12 months.</p>	W396-2	00166
13.	<p>The data-driven and ad-supported online ecosystem benefits consumers and fuels economic growth. Data-driven advertising allows consumers to access content at little or no cost, which surveys show consumers support and prefer to paying for content, and has allowed small businesses to enter the marketplace.</p>	<p>No change has been made in response to this comment, which is interpreted to be an observation rather than a specific recommendation to change these regulations.</p>	W388-1	000112-00113
14.	<p>The AG should clarify how platforms can certify that new or existing privacy settings should be construed as CCPA opt-outs. Businesses should be required to adopt the Global Privacy Control standard or, in the alternative, there should be a</p>	<p>No change has been made in response to this comment. This comment does not appear to relate to the modifications at issue for this 15-day comment period. Rather, it advocates for the need to adopt the Global Privacy Control standard or other standard interface for consumers to exercise their opt-out rights. Section</p>	W382-7 W392-6	00029 00137-00138, 00147

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	<p>standard interface for consumers to exercise their opt-out rights. Research shows that without a standardized control mechanism, businesses are using inconsistent (and in some cases unclear and misleading) opt-out processes. Consumers must repeat opt-out processes for every browser on every device for every business, which is an unreasonable burden and unworkable.</p>	<p>999.315(c) sets forth the requirements for a user-enabled global privacy control that businesses are required to treat as a valid request to opt-out of the sale of their personal information. The OAG considered concerns regarding the lack of standardization in controls and the inconvenience to consumers in repeating opt-out processes for every browser on every device. ISOR, p. 24; FSOR, § 999.315(d). At that time (and before the regulation was approved by OAL), a technical standard that met the requirements set forth in § 999.315(c) had not yet emerged. The Global Privacy Control satisfies the requirements of § 999.315(c) and the OAG encourages businesses to start innovating to support this standard protocol.</p>		
<p align="center">- § 999.315(h)(1)</p>				
<p>15.</p>	<p>Counting the number of steps or clicks to determine whether a business's opt-out method is permissible would be confusing, nonsensical, arbitrary, and devastating to small businesses that use webforms to process CCPA requests. This standard would arbitrarily penalize the use of CAPTCHAs or other means to ensure that the webform is being submitted by a human user rather than bots.</p>	<p>No change has been made in response to this comment. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG's experience in enforcing the CCPA to address businesses using dark patterns to subvert a consumer's choice to opt-out. In drafting this regulation, the OAG considered the wide variety of different industries subject to the regulation, as well as the differing factual scenarios that would apply. Instead of imposing a prescriptive standard based on the number of steps used, the regulation holds the business to a standard the business would create for itself, i.e., the flow process for opting into the sale of data. Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios, but also measurable and clearly enforceable.</p> <p>The regulation does not arbitrarily penalize the use of CAPTCHAs or other means to ensure that the webform is being submitted by a human user; rather, it ensures that the opt-out process is not using a CAPTCHA process to dissuade consumers from opting out. For example, a business that uses a CAPTCHA during the opt-in process</p>	<p>W377-1</p>	<p>00001-00002</p>

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		would also be able to use a CAPTCHA during the opt-out process because the number of steps would cancel each other out.		
16.	Strike section 999.315(h)(1). It would be absurd, impracticable, and an unwarranted overreach by the Attorney General to require that all means of submitting requests involve the same number of steps. The process for submitting a request for a consumer with an established relationship with a business may be simpler than the process for a website visitor who does not have an established relationship and who would have to indicate to the business who they are. These procedures logically and necessarily involve a number of steps.	No change has been made in response to this comment. Civil Code § 1798.185(a)(4)(A) provides the OAG with authority to establish rules and procedures to facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG’s experience in enforcing the CCPA to address businesses using dark patterns to subvert a consumer’s choice to opt-out. Instead of imposing a prescriptive standard based on the number of steps used, the regulation holds the business to a standard the business would create for itself, i.e., the flow process for opting into the sale of data. Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios, but also measurable and clearly enforceable. The OAG is not persuaded by the comment’s assertion that the process for submitting a request to opt-out is more difficult because the business does not have an established relationship with the business. The business may still have to confirm the identity of the consumer when the consumer opts into the sale of personal information.	W377-2	00002
17.	Revise section 999.315(h)(1) to replace the limitation on the number of steps a business may use in its opt-out process with the requirement that section 999.315(b)'s "ease of use by the consumer" includes considering the number of steps an opt-out process takes. The proposed regulation is a specific restriction not contemplated in the CCPA or current regulations. It	No change has been made in response to this comment. Civil Code § 1798.185(a)(4)(A) provides the OAG with authority to establish rules and procedures to facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG’s experience in enforcing the CCPA to address businesses using dark patterns to subvert a consumer’s choice to	W380-1	00013

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	<p>also conflicts with section 999.315(b), which requires businesses to consider both consumers' ease of use and the methods by which the business interacts with consumers.</p>	<p>opt-out. Instead of imposing a prescriptive standard based on the number of steps used, the regulation holds the business to a standard the business would create for itself, i.e., the flow process for opting into the sale of data. Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios, but also measurable and clearly enforceable.</p> <p>The comment's proposed change to make the number of steps discretionary is not more effective in carrying out the purpose and intent of the CCPA. As documented by the Consumer Reports study, there is significant abuse by businesses in this area. Clear guidance with a measurable standard is necessary to curb this abuse. Further, there is no conflict with 999.315(b) because the standard is set by the business with regard to both the opt-out and opt-in processes.</p>		
18.	<p>This example is prescriptive, unnecessary, arbitrary, and does not account for different technological components involved in completing an opt-in and completing an opt-out. As an alternative, this should be a factor in determining whether an opt-out method is permissible, which would be a more flexible approach.</p>	<p>No change has been made in response to this comment. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG's experience in enforcing the CCPA to address businesses' using dark patterns to subvert a consumer's choice to opt-out. In drafting this regulation, the OAG considered the wide variety of different industries subject to the regulation, as well as the differing factual scenarios that would apply. Instead of imposing a prescriptive standard based on the number of steps used, the regulation holds the business to a standard the business would create for itself, i.e., the flow process for opting into the sale of data. Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios, but also measurable and clearly enforceable.</p>	W383-2 W383-3	00083-00084 00084

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		The comment’s proposed change to make the number of steps discretionary is not more effective in carrying out the purpose and intent of the CCPA. As documented by the Consumer Reports study, there is significant abuse by businesses in this area. Clear guidance with a measurable standard is necessary to curb this abuse.		
19.	Simplify section 999.315(h)(1) to address only consumers' opt-in or opt-out actions and be consistent throughout the paragraph; the phrase "opt-in to the sale of personal information after having previously opted out" may create confusion and is subjective.	No change has been made in response to this comment. The regulation is reasonably clear. The phrase “opt-in to the sale of personal information after having previously opted out” is more accurate because the CCPA does not require that businesses obtain opt-in consent for the sale of personal information, except for consumers under the age of 16. Because the use of “opt-in” may encompass the opt-in process for minors and additional considerations relating to parental consent, the language “opt-in to the sale of personal information after having previously opted out” clearly identifies the opt-in process for consumers 16 years and older.	W381-1	00017
20.	Replace "first indication by the consumer to the business of their interest to opt-in" with "a request to opt-in is measured from when the consumer clicks to consent to opt-in" to remove ambiguity and subjectivity about what is the "first indication" and to bring the opt-in language in line with the opt-out language.	No change has been made in response to this comment. The regulation is reasonably clear. The comment’s proposed language is more ambiguous because it is unclear whether “clicks to consent to opt-in” is at the initiation of the opt-in process or the submission/finalization of the opt-in process. If it is at the end of the opt-in process, it would unnecessarily require businesses to shorten their opt-out process.	W381-2	00017-00018
21.	Clarify that a business’s process to validate a user’s identity shall not count in the number of steps to opt-in or opt-out. Requiring parity in the number of opt-in and opt-out steps could incentivize businesses to add steps merely to ensure technical compliance and could present obstacles for businesses employing standard identity verification processes that enhance consumer data security.	No change has been made in response to this comment. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG’s experience in enforcing the CCPA to address businesses’ using dark patterns to subvert a consumer’s choice to opt-out. In drafting this regulation, the OAG considered the wide variety of different industries subject to the regulation, as well as the differing factual scenarios that would apply. Instead of imposing a prescriptive standard based on the number of steps used, the regulation holds the business to a standard the business would create for itself, i.e., the flow process for opting into the sale of data.	W385-2	00092-00093

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		<p>Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios, but also measurable and clearly enforceable.</p> <p>The comment’s criticism that the regulation could present obstacles for businesses employing standard identity verification processes is not convincing because a request to opt-out need not be a verifiable consumer request. The comment provides no further evidence or discussion that explains a situation where a business needs to do more to verify a consumer who wants to opt-out than a consumer who wants to opt-in.</p>		
- § 999.315(h)(2)				
22.	Strike section 999.315(h)(2). Banning "confusing language" is overbroad and lacks statutory authorization. It also raises due process and First Amendment concerns because it prohibits an undefined category of speech, since there is no guidance as to what is or could be "confusing" to consumers.	No change has been made in response to this comment. Civil Code § 1798.185(a)(4) provides the AG with authority to facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information and subsection (a)(6) provides the AG with authority to establish rules and procedures necessary to ensure that businesses provide information in a manner that may be easily understood by the average consumer. The term “confusing” is reasonably clear and should be understood by the plain language of the word. Moreover, the proposed regulation provides businesses with clear guidance about what would be “confusing” through the example of the use of double negatives.	W380-2	00013
- § 999.315(h)(3)				
23.	Strike or revise section 999.315(h)(3) to allow businesses to provide a reasonable degree of notice to the consumer regarding information that could be important, relevant, and informative to them, including info about partial opt-out options. This is a prohibition on content, not an illustrative example of "ease of use", and without specific definitions or limitations, this prohibition could	No change has been made in response to this comment. The proposed regulation is not a prohibition on content and serves a purpose unrelated to the content of the expression. It is also reasonably clear in its definitions and limitations. As indicated by the phrase “[e]xcept as permitted by these regulations,” the proposed regulation allows businesses to provide notice to consumers about partial opt-out options and other information about their right to opt-out. (See §§ 999.306, 999.315(d).) The proposed regulation only	W380-3 W383-3 W385-3 W386-4 W388-2 W390-2 W391-3 W391-5	00014 00084 00093 00099-00100 00113-00114 00128 00130-00132 00130-00132

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	discourage businesses from including helpful, explanatory language to help consumers understand their options and what effect opt-outs have. It limits businesses' ability to provide more transparency and helpful information to consumers.	prohibits businesses from requiring consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request. It does not prohibit the provision of that information elsewhere and does not prohibit a link to that information that consumers may choose to, but not be required to, click for more information. Requiring consumers to click through or listen to these reasons is an example of a method that has the purpose or substantial effect of subverting or impairing consumer choice. As documented by the Consumer Reports study, there is already abuse by businesses in this area. The proposed regulation is narrowly tailored to advance the significant governmental interest of protecting consumers from burdensome anti-consumer or anti-privacy practices while leaving open alternative channels for the communication of information about why consumers should not submit a request to opt-out. The comment's proposed change to allow businesses a reasonable degree of notice is not more effective in carrying out the purpose and intent of the CCPA. Clear guidance with a measurable standard is necessary to curb this abuse.	W395-1	00159
24.	Strike section 999.315(h)(3). The regulation infringes on businesses' First and Fourteenth Amendment right to commercial speech. It is a content restriction that does not benefit consumers or advance a substantial interest. It unduly limits the way that businesses may communicate with consumers, does not directly advance the interest in removing perceived impediments to opt-outs and other requirements already do so, and is not narrowly tailored. It is also unclear what amount of information, or what method of presentation, could constitute a violation and does not provide any guidance on what "reasons not to opt out" means.	No change has been made in response to this comment. See response #22. Additionally, the proposed regulation meets the standard applicable to commercial speech. There is a clear and significant government interest in protecting the privacy of consumers and in protecting consumers from dark patterns, which have the purpose or substantial effect of subverting or impairing consumer choice. The proposed regulation reasonably addresses these significant interests, as it streamlines the opt-out process while businesses may display this information elsewhere.	W380-4 W388-2 W388-3 W391-4 W395-1	00014 00113-00114 00114-00115 00130-00132 00159

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
- § 999.315(h)(4)				
25.	Strike section 999.315(h)(4). It exceeds the scope of the CCPA, as the CCPA does not restrict what information businesses can request to effectuate a consumer's opt-out and already prohibits businesses from using personal information obtained for verification of a request for any other purpose.	No change has been made in response to this comment. Civil Code § 1798.185(a)(4)(A) provides the OAG with authority to establish rules and procedures to facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG's experience in enforcing the CCPA to address businesses' use of dark patterns to subvert a consumer's choice to opt-out. Businesses should not use the opt-out process to obtain additional personal information from consumers when it is unnecessary to carry out the request to opt-out especially in light of the fact that requests to opt-out need not be verified. Seeking additional personal information may deter or encumber consumers seeking to exercise their right to opt-out.	W380-5	00014
26.	Strike section 999.315(h)(4) because it is vague and lacks detail. It raises due process concerns because there is no guidance on how a business is expected to assess whether information is necessary to implement a request. Without guidance about what information is considered "not necessary", businesses cannot assess whether they are in compliance with this standard. Imposing a restriction on required data points makes it more difficult for businesses to match opt-out requests to data on a particular consumer.	No change has been made in response to this comment. The regulation is reasonably clear and should be understood from the plain meaning of the words. The regulation is meant to apply to a wide-range of factual situations and across industries. It does not impose a prescriptive restriction on required data points, but rather, places a performance standard on businesses to only require personal information that is necessary for them to implement the request. The regulation applies the internationally recognized fair information practice principle ("FIPP") of data minimization, i.e., to only collect data directly relevant and necessary to accomplish the specified purpose. If a business cannot explain why the personal information is necessary for them to implement the request to opt-out, they should not require it from consumers.	W380-6 W390-3	00014-00015 00128
- § 999.315(h)(5)				
27.	Strike section 999.315(h)(5). It would arbitrarily penalize businesses for minor procedural or technical issues and would allow the Attorney General to set arbitrary, undefined expectations for what constitutes excessive searching or	No change has been made in response to this comment. The regulation does not arbitrarily penalize businesses; Civil Code § 1798.155(b) provides businesses with a 30-day cure period before the imposition of legal action, including penalties. In addition, this regulation, as well as § 999.306(b)(1) and (c), are reasonably clear	W377-3	00002

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	scrolling. For example, a straightforward "Do Not Sell" webpage may require a fair bit of scrolling if a consumer accesses the page from a mobile phone rather than a desktop computer.	that upon clicking on the link, the consumer should be directed to information about their right to opt-out, the interactive form by which they can submit their request, and instructions for any other method by which the consumer can submit their request. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG's experience enforcing the CCPA to address businesses' use of dark patterns to subvert a consumer's choice to opt-out. It is necessary to address abuses already appearing in the marketplace.		
28.	Strike section 999.315(h)(5). It is confusing because it is unclear as to what counts as a "privacy policy or similar document or website." The CCPA and current regulations already provides guidance on the placement of the "Do Not Sell My Personal Information" link. It also raises due process and First Amendment concerns because it prohibits the inclusion of information alongside the opt-out mechanism and without clarification about what is objectionable, businesses cannot comply with this restriction.	No change has been made in response to this comment. The regulation is reasonably clear and should be understood from the plain meaning of the words. There are no due process issues because this regulation, as well as § 999.306(b)(1) and (c), are reasonably clear that upon clicking on the "Do Not Sell My Personal Information" link, the consumer should be directed to information about their right to opt-out, the interactive form by which they can submit their request, and instructions for any other method by which the consumer can submit their request. The language "privacy policy or similar document or webpage" is consistent with § 999.306(b), which allows businesses to meet their obligations to post a notice of opt-out by directing consumers to the section of their privacy policy that contains the same information. As explained in the 2nd Addendum to the FSOR, the regulation was made in response to comments raised during the rulemaking process and the OAG's experience enforcing the CCPA to address businesses' use of dark patterns to subvert a consumer's choice to opt-out. It is necessary to address the abuses already appearing in the marketplace. Further, there are no First Amendment concerns because the proposed regulation is a valid time-place-manner restriction. The proposed regulation is content-neutral because it is justified without reference to the content of any given privacy policy. Businesses may link to or otherwise display their privacy policy alongside the opt-out mechanism. The proposed regulation seeks to protect consumers from being forced to search or scroll through text to find the opt-out	W380-7	00015

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		mechanism, which may have the purpose or substantial effect of subverting or impairing consumer choice. The proposed regulation is narrowly tailored to serve the significant governmental interest of protecting consumer privacy and enabling consumers to exercise their rights under the CCPA. It does not prohibit any content that businesses may wish to include. It does not preclude other means by which businesses may make their privacy policies known to consumers, including through the use of additional hyperlinks. The proposed regulation thus leaves open alternative channels of communication for businesses to convey information.		
29.	Clarify how this section aligns with the existing requirements in Civil Code §§ 1798.115(d) and 1798.120(b).	No change has been made in response to this comment. It is unclear what the comment is saying. Section 999.315(h)(5) pertains to a business’s method for submitting requests to opt-out, while Civil Code § 1798.115(d) and 1798.120(b) pertains to third parties selling personal information. To the extent that the commenter is asking whether a business’s failure to comply with this regulation would impact whether the third party can sell personal information received from the business, such would be a fact-specific determination.	W386-6	00100
§ 999.326. Authorized Agent				
- § 999.326(a)				
30.	Supports the proposed change as a straightforward and sensible clarification of the existing text. It promotes more choice and flexibility in agent authorization practices while allowing businesses to require consumers to verify their identity as necessary. Supports efforts to make consumers’ interactions with businesses through the use of authorized agents smoother.	The OAG appreciates this comment of support. No change has been made in response to this comment. The comment concurred with the proposed regulations, so no further response is required.	W377-4 W383-4 W389-4	00002 00084 00124
31.	Supports the proposed regulation, which upholds the use of authorized agents while ensuring that consumers' privacy and security is protected. It is appropriate to allow businesses to require additional identity verification only if an authorized	The OAG appreciates this comment of support. No change has been made in response to this comment. The comment concurred with the proposed regulations, so no further response is required.	W382-4	00025-00026

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	<p>agent cannot present proof that it holds a consumer's power of attorney, as allowing multiple businesses to require a consumer to submit additional verification would render the authorized agent provision impracticable for consumers. The "good-faith, reasonable, and documented belief" that a request is fraudulent is an appropriate standard because it allows businesses to reject fraudulent opt-outs without putting additional verification burdens on consumers.</p>			
32.	<p>The proposed regulation may highly restrict the efficiency and opportunity for consumers to designate an authorized agent and places unnecessarily hurdles between authorized agents and the effective and efficient control of private information. Businesses should implement a dedicated communication channel with authorized agents, preferably an email address; authorized agents could not manage privacy requests efficiently if forced to use web forms or postal mail.</p>	<p>No change has been made in response to this comment. In drafting these regulations, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer's statutory right to use an authorized agent as required by the law. The OAG determined that giving businesses the discretion to require the consumer to verify their identity directly with the business allows businesses to utilize their existing verification processes and complies with general privacy principles to not share one's security credentials (login ID and passwords) with others. ISOR, p. 33. Authorized agents will serve to facilitate requests and responses, but they themselves will not be allowed to collect or amass consumers' sensitive information for the purposes of verification. ISOR, p. 33. Giving businesses the discretion to require the consumer to directly confirm with the business that they provided the authorized agent permission to submit the requests also allows businesses to authenticate the signed permission. FSOR at § 999.326. Businesses have discretion to determine which requirement, if any, is warranted based on the factors set forth in §§ 999.323(b), 999.324, and 999.325 of these regulations. The comment's proposal to require a dedicated communication channel for authorized agents is not more effective in carrying out the purpose and intent of the CCPA. Given the wide variety of different industries subject to the CCPA, there are many different ways in which the business can engage authorized agents. At this</p>	W379-1 W389-7	00008 00125

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		time, the OAG does not believe that prescribing a dedicated email address is the most effective manner in facilitating requests made by authorized agents. It may unnecessarily increase costs for businesses and may raise security concerns. However, the OAG will continue to evaluate the need for additional regulations as part of its ongoing rulemaking authority.		
33.	Allowing a business to contact the consumer directly for additional identity verification would impair consumers' rights by making designation of an authorized agent less practicable and by leading to additional processes and unnecessary delays to the processing of the consumer's original request. Consumers that designate authorized agents do so to avoid having to manage such requests themselves and to avoid receiving numerous emails from businesses to confirm their identity or the validity of their request.	No change has been made in response to this comment. The regulations are meant to be robust and applicable to many factual situations and across industries. In drafting these regulations, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer's statutory right to use an authorized agent as required by the law. The OAG determined that giving businesses the discretion to require consumers to verify their identity directly with the business or directly confirm that they provided the authorized agent their permission to submit their request is more effective in carrying out the purpose and intent of the CCPA than the comment's proposed change because it balances consumers' ability to exercise their rights while preventing fraud and abuse. Disclosing personal information, especially sensitive personal information, into the wrong hands may cause grave harm to consumers in certain circumstances. Businesses should have discretion to determine whether additional verification requirements are warranted based on the factors set forth in §§ 999.323(b), 999.324, and 999.325 of these regulations.	W379-2 W389-5	00008 00124
34.	Narrow the scope of the regulation to allow businesses to require the consumer to verify their own identity directly with the business only "in case the authorized agent has not provided reasonable proof that the authorized agent has previously verified the consumer's identity" and to allow businesses to require the consumer to directly confirm with the business that they provided the authorized agent permission to submit the request only "in case the authorized	No change has been made in response to this comment. The regulations are meant to be robust and applicable to many factual situations and across industries. In drafting these regulations, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer's statutory right to use an authorized agent as required by the law. The OAG determined that giving businesses the discretion to require consumers to verify their identity directly with the business or directly confirm that they provided the authorized agent their permission to submit their request is more effective in carrying out	W379-3 W389-8	00008-00009 00125

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	agent has not provided reasonable proof of the existence of a signed mandate."	the purpose and intent of the CCPA than the comment's proposed change because it balances consumers' ability to exercise their rights while preventing fraud and abuse. Disclosing personal information, especially sensitive personal information, into the wrong hands may cause grave harm to consumers in certain circumstances. Businesses should have discretion to determine whether additional verification requirements are warranted based on the factors set forth in §§ 999.323(b), 999.324, and 999.325 of these regulations.		
35.	A consumer's "signed permission to submit request" should be deemed sufficient unless there are reasonable grounds to believe otherwise. The Attorney General should prepare a "signed permission" template. This would balance between different regulatory objectives, save time and cost, and reduce information asymmetries.	No change has been made in response to this comment. The regulations are meant to be robust and applicable to many factual situations and across industries. In drafting these regulations, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer's statutory right to use an authorized agent as required by the law. The OAG determined that giving businesses the discretion to require consumers to verify their identity directly with the business or directly confirm that they provided the authorized agent their permission to submit their request is more effective in carrying out the purpose and intent of the CCPA than the comment's proposed change because it balances consumers' ability to exercise their rights while preventing fraud and abuse. Disclosing personal information, especially sensitive personal information, into the wrong hands may cause grave harm to consumers in certain circumstances. Businesses should have discretion to determine whether additional verification requirements are warranted based on the factors set forth in §§ 999.323(b), 999.324, and 999.325 of these regulations. The comment's proposal to prepare a "signed permission" template is not more effective in carrying out the purpose and intent of the CCPA because it does not take into consideration circumstances where the sensitive nature of the personal information and the potential harm to consumers by an unauthorized disclosure may warrant additional verification. However, the OAG will continue to evaluate the need for additional regulations as part of its ongoing rulemaking authority.	W389-6	00124-00125

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
36.	Strike the proposed modification and return to the previous version. The proposed modification would impede the ability of businesses to obtain verification in instances of suspected fraud and thus undermines consumer data security and is counter to the CCPA’s other authentication requirements. Businesses should have the ability to both (1) directly verify a consumer’s identity and (2) verify that the consumer provided authorization to the agent submitting the request. Businesses should not be required to choose between the two.	No change has been made in response to this comment. In drafting these regulations, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer’s statutory right to use an authorized agent as required by the law. The OAG determined that giving businesses the discretion to require consumers to verify their identity directly with the business or directly confirm that they provided the authorized agent their permission to submit their request is more effective in carrying out the purpose and intent of the CCPA than the comment’s proposed change because it balances consumers’ ability to exercise their rights while preventing fraud and abuse. The comment’s proposed change is not as effective and less burdensome to affect private persons because it would allow businesses to create unnecessary barriers to the use of an authorized agent. If a consumer verifies their own identity with the business, it would be unnecessary for the consumer to also directly confirm that they provided the authorized agent their permission, and vice versa.	W385-4 W386-5 W387-3 W395-5	00093-00094 00100 00108-00109 00161
37.	Businesses should be allowed to require authorized agents to verify their own identities. Otherwise, fraudsters could pose as authorized agents to access consumers’ personal information.	No change has been made in response to this comment. The comment’s proposed change is not as effective and less burdensome to affected private persons than the adopted regulation. In drafting these regulations, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer’s statutory right to use an authorized agent as required by the law. The OAG determined that requiring the consumer to verify their identity directly with the business allows businesses to utilize their existing verification processes and complies with general privacy principles to not share one’s security credentials (login ID and passwords) with others. ISOR, p. 33. Authorized agents will serve to facilitate requests and responses, but they themselves will not be allowed to collect or amass consumers’ sensitive information for the purposes of verification. ISOR, p. 33. The OAG determined that requiring the consumer to directly confirm with the business that they provided the authorized agent permission to submit the requests allows businesses to authenticate the signed permission.	W387-2	00107-00108

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		FSOR at § 999.326. Businesses have discretion to determine whether this requirement is warranted based on the factors set forth in §§ 999.323(b), 999.324, and 999.325 of these regulations. In light of these protections for the consumer, the OAG does not see the utility of requiring authorized agent to verify their own identities. Requiring so would place an unnecessary burden on consumers who seek to use an authorized agent to submit a request under the CCPA.		
38.	The proposed modifications do not provide sufficient consumer protection from potential deception by authorized agents and should be modified to equalize the notice requirements placed on businesses and authorized agents. Authorized agents are subject to little to no rules regarding their communications with consumers, while businesses are subject to onerous, highly restrictive requirements.	No change has been made in response to this comment. The comment does not provide sufficient specificity to the OAG to make any modifications to the text. The comment provides no evidence that authorized agents are deceiving consumers such that a regulation is necessary. Further, in drafting these regulations, the OAG weighed the risk of fraud and misuse of consumer information and the burden to the business with the consumer’s statutory right to use an authorized agent as required by the law. The comment appears to object to the CCPA, which gives consumers the statutory right to use authorized agents to submit requests, not the proposed regulation. Moreover, the regulations do place restrictions on authorized agents to protect consumers. Section 999.326(c) requires agents to implement and maintain reasonable security procedures and practices to protect consumers’ information, and § 999.326(d) prohibits them from using personal information, or any information from or about the consumer, for any purpose other than to fulfill the consumer’s requests, for verification, or for fraud prevention.	W388-4	00115-00116
39.	Clarify what “proof” is sufficient to evidence “signed permission to submit the request.”	No change has been made in response to this comment. The regulation is reasonably clear and should be understood from the plain meaning of the words. A business may require an authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. Section 999.301, subd. (u), defines “signed” for purposes of these regulations.	W386-7	00100
§ 999.332. Notices to Consumers Under 16 Years of Age				
- § 999.332(a)				
40.	Recommends deleting "and/or" and replacing with "or."	No change has been made in response to this comment. The comment provides no reason why “and/or” should be replaced by	W389-9	00125

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		<p>“or.” Moreover, the suggested language is not more effective than the language proposed. This language conveys that the provision applies to businesses subject to both or either section 999.330 and 999.331 and is provided to achieve clarity.</p>		
General Comment Regarding All Modifications				
41.	<p>The proposed amendments are unlawful and invalid because they violate the California APA; the Attorney General must withdraw them and restart a new notice period. Government Code section 11346.4(b) states that a Notice of Proposed Action is valid for one year, and these proposed amendments were published 367 days after the original Notice of Proposed Action. None of the amended provisions modify the subdivisions that were originally withdrawn and, even if they did, they were not resubmitted to the Office of Administrative Law for review within the one-year period specified in Government Code section 11346.4(b).</p>	<p>No change has been made in response to this comment. The proposed modifications to the regulations do not violate the California Administrative Procedures Act. The Governor’s Executive Orders N-40-20 and N-66-20 extended the deadline to complete and transmit a rulemaking package to the Office of Administrative Law (OAL) by 120 calendar days. Accordingly, the OAG has until February 7, 2021 to complete and submit its rulemaking package to OAL.</p>	W386-1	00097-00098
42.	<p>Adding new requirements makes compliance more difficult for businesses and impacts consumers’ ability to exercise their CCPA rights. The Attorney General should stop rulemaking for a while to allow businesses to implement the current regulations and to allow regulators to identify true challenges to the new rules.</p>	<p>No change has been made in response to this comment. The OAG disagrees with the comment. In drafting these regulations, the OAG has considered the burden on businesses as well as consumers’ ability to exercise their CCPA rights. As set forth in the 2nd Addendum to the FSOR, the proposed regulations provide guidance to businesses and bring clarity whether there may have been some ambiguity. They also address real barriers consumers face when exercising their CCPA rights.</p>	W391-1	00130
COMMENTS NOT DIRECTED AT 15-DAY MODIFIED TEXT				
43.	<p>The Attorney General should require businesses to confirm they have honored opt-out requests. Without this, consumers do not know whether their opt-outs were effectuated.</p>	<p>No change has been made in response to this comment. This comment relates to § 999.315, subd. (e), which requires a business to comply with an opt-out request within 15 days. The modifications here involve § 999.315, subd. (h), which relates to obstacles employed by businesses to make the opt-out process difficult for consumers to use. However, the OAG appreciates the comment and</p>	W382-3	00025

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
		will consider whether additional regulations are necessary in the future.		
44.	Clarify the definition of "sale" and tighten protections regarding service providers to ensure that consumers can opt-out of behavioral advertising: 1) Define "sale" in § 999.301 as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration, or otherwise for a commercial purpose"; 2) revise § 999.314(d) to clarify that businesses cannot share personal information with a service provider for behavior advertising if the consumer has submitted an opt-out; and 3) prohibit service providers from combining "the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers."	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. The modifications do not affect §§ 999.301 or 999.314.	W382-5	00026-00028
45.	Clarify that financial incentives in markets that lack competition is an unfair and usurious practice. Discriminatory treatment should be presumed where markets are consolidated and consumers lack choices.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W382-6	00028
46.	Delete section 999.307(b)(5) and draft regulations concerning the exceptions for trade secrets, intellectual property rights, and other possible exceptions needed to comply with state and federal law, as mandated by § 1798.185(a)(3). The	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W394-1	00153-00154

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	Legislature tasked the Attorney General with adopting regulations regarding these exceptions, and the Attorney General has failed to do so.			
47.	Strike the Web Content Accessibility Guidelines (“WCAG”) requirements. The Attorney General has overstepped his authority; the U.S. Department of Justice has stated that public accommodations have flexibility in how to comply with the ADA, and the Ninth Circuit has held that the ADA was intended to give businesses maximum flexibility in meeting its requirements. Given that the regulations have still not been finalized and the impact of the COVID-19 pandemic, it does not make sense to introduce new WCAG requirements when these regulations complicate the question of what the regulations require and create new, substantial costs for online companies. There is also no evidence that these WCAG requirements are really “generally recognized industry standards” and the Department of Justice and the Ninth Circuit hold positions to the contrary. As stated in the previous comment, these requirements are unconstitutional and make it practically impossible for companies to comply because they cannot provide simple notices when the rules behind them are so complex.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W394-3	00155-00157
48.	The Attorney General should create and maintain a “Do Not Sell” database, similar to the Federal Trade Commission’s “Do Not Call” list, and effectively become an authorized agent under section 999.326. This would allow consumers to conveniently exercise their CCPA rights efficiently and easily rather than submit opt-out requests to each data broker separately. The database would	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W396-3	00166-00168

FSOR APPENDIX G: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING THIRD 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_3RD15DAY_)
	include identifiers such as name, address, and phone number. Consumers would trust the Attorney General more than browser plug-ins or other technologies to hold their personal information; businesses could have a single centralized list to automate checking against to ensure compliance rather than receiving random requests; and the Attorney General can properly authenticate users.			
49.	The Attorney General should hold a series of meetings with stakeholders to develop best-practice recommendations to ensure that tools for CCPA compliance are legally compliant.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W396-4	00168-00171

FSOR APPENDIX H: LIST OF COMMENTERS FROM 3RD 15 DAY PERIOD

Name	Organization	Comment #	Response #
Anonymous		W377-1	15
		W377-2	16
		W377-3	27
		W377-4	30
Adam Schwartz	Electronic Frontier Foundation	W378-1	7
Zoe Vilain, Pierre Valade	Jumbo Privacy	W379-1	32
		W379-2	33
		W379-3	34
Eric Ellman	Consumer Data Industry Association	W380-1	17
		W380-2	22
		W380-3	23
		W380-4	24
		W380-5	25
		W380-6	26
		W380-7	28
Melissa MacGregor, Kimberly Chamberlain	Securities Industry and Financial Markets Association	W381-1	19
		W381-2	20
Maureen Mahoney	Consumer Reports	W382-1	7
		W382-2	9
		W382-3	43
		W382-4	31
		W382-5	44
		W382-6	45
		W382-7	14
Susan Kammerer, Jeremy Merz	American Property Casualty Insurance Association	W383-1	1
		W383-2	18
		W383-3	18, 23
		W383-4	30
Dale Smith	PrivacyCheq	W384-1	2

Name	Organization	Comment #	Response #
		W384-2	9
Emily Emery, Brigitte Schmidt Gwyn, Rita Cohen	The Association of Magazine Media	W385-1	2
		W385-2	21
		W385-3	23
		W385-4	36
Shoeb Mohammed, Leslie Leder	California Chamber of Commerce	W386-1	41
		W386-2	1
		W386-3	3
		W386-4	23
		W386-5	36
		W386-6	29
		W386-7	39
Melanie Tiano, Gerard Keegan	CTIA	W387-1	1
		W387-2	37
		W387-3	36
Allaire Monticollo, Dan Jaffe, Christopher Oswald, David LeDuc, Lou Mastria, Alison Pepper, David Grimaldi, Clark Rector	Association of National Advertisers, American Association of Advertising Agencies, Interactive Advertising Bureau, American Advertising Federation, Digital Advertising Alliance, Network Advertising Initiative, Venable LLP	W388-1	13
		W388-2	23, 24
		W388-3	24
		W388-4	38
		W388-5	6
Paul Jurcys, Markus Lampinen	Prifina, Inc.	W389-1	5
		W389-2	4
		W389-3	8
		W389-4	30
		W389-5	33
		W389-6	35
		W389-7	32

FSOR APPENDIX H: LIST OF COMMENTERS FROM 3RD 15 DAY PERIOD

Name	Organization	Comment #	Response #
		W389-8	34
		W389-9	40
Courtney Jensen	TechNet	W390-1	1
		W390-2	23
		W390-3	26
Dylan Hoffman	Internet Association	W391-1	42
		W391-2	10
		W391-3	23
		W391-4	24
		W391-5	23
Jennifer King, Adriana Stephan, Emilia Porubcin, Claudia Bobadilla, Morgan Livingston	Stanford Law School	W392-1	11
		W392-2	11
		W392-3	11
		W392-4	11
		W392-5	11
		W392-6	14
Rachel Nemeth, Michael Petricone	Consumer Technology Association	W393-1	1
Javier Bastidas, Lara DeCaro	Leland, Parachini, Steinberg, Matzger & Melnick LLP	W394-1	46
		W394-2	9
		W394-3	47
Jim Halpert	State Privacy and Security Coalition, Inc.	W395-1	23, 24
		W395-2	1
		W395-3	3
		W395-4	2
		W395-5	36
Maggie Feng, Zeeshan Sadiq Khan, Bingxuan Luo, Xiaofei Ma, Arjita Mahajan, Aleecia McDonald	Carnegie Mellon	W396-1	7
		W396-2	12
		W396-3	48
		W396-4	49

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information				
- § 999.306(b)(3)				
1.	Supports the proposed modification. It is a useful clarification and less onerous than the originally proposed language.	The OAG appreciates this comment of support. No change has been made in response to this comment. The comment concurred with the proposed regulations, so no further response is required.	W397-1 W402-1 W412-1	00001 00039 00086
2.	The proposed modifications are more restrictive and prescriptive than the CCPA, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. The regulations already provide guidance and so the modifications are unnecessary and overly prescriptive. The specificity of the examples could result in over-notification and do not account for different contexts. The OAG should remove the proposed illustrative examples associated with brick-and-mortar stores and explicitly enable businesses communicating with consumers by phone to direct them to an online notice.	No change has been made in response to this comment. The OAG does not agree that providing these illustrative examples are overly prescriptive or unnecessary. This regulation provides guidance on how to make information about a consumer's right to opt-out reasonably accessible to consumers who interact with businesses offline so that they have the same opportunity to exercise their right to opt-out as consumers interacting with the business online. The examples illustrate some ways in which a business may inform consumers by an offline method and consider as a factor when and how the consumer is providing their personal information. The examples are neither exclusive nor exhaustive. Businesses have the flexibility to inform consumers in different ways provided that they are facilitating consumers' awareness of their right to opt-out. The comment also misconstrues the requirement that businesses must read the full notice aloud over the phone. The modification clarifies that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out and how to submit a request to opt-out. The OAG does not agree that directing the consumer to an online notice is sufficient; to avoid consumer confusion, businesses may need to also provide context for the notice, i.e., that it pertains to the consumer's right to opt-out and how to do it. The regulation does not prohibit directing the consumer to a webpage for more information provided that the business gives the consumer the appropriate context for what the webpage is about, i.e., that they have a right to opt-out and that they can do so through the webpage.	W401-6	00035-00037
3.	The OAG should clarify in its modifications that in instances where personal information is collected through a printed form that is to be	No change has been made in response to this comment. This regulation provides guidance on how to make information about a consumer's right to opt-out reasonably accessible to consumers who	W406-1	00057-00058

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
	mailed back to the company that the offline notice may include a web address that the customer can access to opt-out of the sale of their personal information.	interact with businesses offline so that they have the same opportunity to exercise their right to opt-out as consumers interacting with the business online. The examples illustrate some ways in which a business may inform consumers by an offline method and consider as a factor when and how the consumer is providing their personal information. The examples are neither exclusive nor exhaustive. Businesses have the flexibility to inform consumers in different ways provided that they informing the consumer of their right to opt-out and how to submit a request to opt-out. Simply including a web address on a printed form with no additional context may not be sufficient.		
4.	Changing the regulation to apply to the sale of personal information instead of collection narrows the scope of covered interactions with consumers. All people should be notified of information collection whether it's intended to be "sold" or used by the business. Selling is more ambiguous than collection and so businesses may adopt a cramped definition of sale to avoid their obligations. Security risks from data breaches exist for the consumer just from the collection of the personal information. Also, the CPRA restricts the "sharing" of user data so there may be conflicting standards.	No change has been made in response to this comment. The comment appears to mistake the notice of right to opt-out of the sale of personal information with the notice at collection. This regulation pertains to the notice of right to opt-out of sale of personal information. If the business is not selling the personal information collected offline, there is no need to notify the consumer of the right to opt-out of sale. Notifying them of a right that would not apply to them may in fact be confusing to the consumer. As to the comment's concern that all people should be notified of information collection, Civil Code § 1798.100(b) already requires a business that collects a consumer's personal information to inform consumers, at or before the point of collection, as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. Section 999.305 sets forth the requirements businesses are to follow with regard to this notice at collection. Consumers will still be notified even if the business does not sell the consumer's personal information because the obligation to provide a notice at collection is separate from the obligation to provide a notice of right to opt-out. To the extent that the comment takes the position that the consumer should have the ability to opt-out of the collection or sharing of personal information, the comment objects to the CCPA, not the proposed regulation. Civil Code § 1798.140(t) defines sale and that definition is adopted in the regulations. See § 999.301. To the extent	W410-2	00076-00077

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
		that the CPRA alters businesses’ obligations with regard to the sale or sharing of personal information, it is not yet in effect. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020) at § 31.)		
- § 999.306(f)				
5.	Supports the AG’s button design and recommends that it be finalized as proposed.	The OAG appreciates this comment of support. No change has been made in response to this comment. The comment concurred with the proposed regulations, so no further response is required.	W398-1 W411-1	00007-00008 00084
6.	The proposed button is ugly and is unlikely to help the average consumer grasp the intended significance of the graphic and how it relates to privacy or the opting-out of the sale of their personal information.	No change has been made in response to this comment. The OAG selected the blue toggle design after studying and testing a number of different graphics with consumers and finding that the blue toggle design performed much better than the other graphics in communicating that a consumer has choices over how websites can use their personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020); Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020). The comment has not proposed any alternative design that would be more effective in implementing the required mandate that the OAG adopt regulations for the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the right to opt-out. Civil Code, § 1798.185, subd. (a)(4)(C).	W397-2	00001
7.	It is unclear whether the visual graphic is a “button” or an “icon.” The distinction is important from a web design perspective because buttons have their own rules and best practices, especially when it comes to programming for accessibility. An icon, by comparison, is a visual symbol of wayfinding and identifying and appears to be what the AG’s office had in mind. The AG should clarify that it’s an icon because the regulations are confusing as written.	Accept in part. The OAG has made the non-substantive change of replacing the word “button” with “icon” for accuracy, consistency, and clarity. As set forth in the Second Addendum to the Final Statement of Reasons and the studies supporting the graphic’s selection, the proposed opt-out button design was not intended to convey a specific meaning for the purpose of web design or to connote the functionality of a toggle. Rather, it is an icon or visual graphic that businesses shall use to convey the presence of a choice and to build awareness about the consumer’s right to opt-out of the sale of personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by	W403-1	00041-00043

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
		CCPA (February 4, 2020), pp. 1-3; see also Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020).		
8.	The proposed button is not compatible with screen readers or other assistive technologies used by people with disabilities. The study that informed this decision doesn't seem to have sought out any participants with disabilities.	No change has been made in response to this comment. The OAG has made the non-substantive change of replacing the word “button” with “icon” for accuracy, consistency, and clarity. As set forth in the Second Addendum to the Final Statement of Reasons and the studies supporting the graphic’s selection, the proposed opt-out button design was not intended to convey a specific meaning for the purpose of web design or to connote the functionality of a toggle. Rather, it is an icon or visual graphic that businesses shall use to convey the presence of a choice and to build awareness about the consumer’s right to opt-out of the sale of personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020), pp. 1-3; see also Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020). The clarification that the graphic is an icon addresses how it should be read with screen readers and other assistive technologies. Also, the Cranor study did consider accessibility barriers and tested both grayscale and colored versions of the different icons to ensure that color was not a factor in the participants’ decisions. See Cranor, et al. (February 4, 2020), p. 8 at fn. 6, and p. 36.	W397-3 W403-3	00001 00042-00043
9.	The wording of the provision is unclear. 999.306(f)(1) suggests that it is optional (“may be used in addition to posting”), while 999.306(f)(2) implies that it is mandatory (“Where a business... shall be added”). Some comments suggest that it be made optional and other comments suggest that it be mandatory.	No change has been made in response to this comment. The regulation is reasonably clear. Use of the icon is optional. The OAG developed the icon to provide an opportunity for businesses to promote consumer awareness of their privacy rights under the CCPA. If a business wants to promote a consumer’s privacy rights by using the icon, the regulation requires the icon to be placed to the left of the “Do Not Sell My Personal Information” link. This location is mandatory because it promotes awareness of the consumer’s right to opt out of the sale of their personal information. Businesses may use the icon in additional locations at their discretion. Additional uses of the design will facilitate multiple pathways for the consumer to exercise their right to opt-out. See Habib, et al., “It’s a scavenger hunt”: Usability of Websites’ Opt-Out and Data Deletion Choices, CHI ’20: Proceedings of	W397-4 W398-2 W399-1 W400-2 W401-1 W402-5 W405-1 W408-1 W409-1 W412-4	00001 00008-00009 00023 00025-00026 00031-00032 00040 00051-00052 00068-00069 00072-00073 00086, 00088

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
		the 2020 CHI Conference on Human Factors in Computing Systems, April 2020, Honolulu, HI, USA, at pg. 7.		
10.	The AG should provide flexibility for businesses to use alternative, industry-developed icons, such as DAA YourAdChoices, that signal the right to opt-out of personal information sales to CA consumers. The AG should allow the marketplace to determine the best opt-out button approach.	No change has been made in response to this comment. This comment objects to the underlying statute, which requires the OAG to adopt regulations for the development and use of an uniform opt-out logo or button. The OAG selected the blue toggle design after studying and testing a number of different graphics with consumers and finding that the blue toggle design performed much better than the other graphics in communicating a consumer’s choice over how websites can use their personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020); Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020). The comment’s proposed change to allow the marketplace to determine the best opt-out button approach is not as effective and less burdensome to affected persons than the adopted regulation. Consumer testing demonstrated that other icons in the marketplace, including the DAA AdChoices icon, were not widely recognized and failed to communicate the ability to make choices or opt-out. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA, <i>supra</i> , at p. 3. Moreover, the regulations do not prohibit businesses from also using alternative industry-developed icons, provided that they comply with the regulations and do not confuse or mislead the consumer.	W401-2	00032
11.	The optional button is likely to lead to consumer confusion due to lack of uniformity of use. The AG should delete this proposed addition, particularly at this late stage.	No change has been made in response to this comment. The OAG developed the icon to provide an opportunity for businesses to promote consumer awareness of their privacy rights under the CCPA. If a business wants to promote a consumer’s privacy rights by using the icon, the regulation requires the icon to be placed to the left of the “Do Not Sell My Personal Information” link. This location is mandatory because it promotes awareness of the consumer’s right to opt out of the sale of their personal information. Businesses may use the icon in additional locations at their discretion. The comment’s proposed	W404-1	00045

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
		change to delete § 999.306(f) is not more effective in carrying out the purpose and intent of the CCPA. Civil Code § 1798.185(a)(4)(C) requires the OAG to develop a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information. The OAG selected the blue toggle design after studying and testing a number of different graphics with consumers and finding that the blue toggle design performed much better than the other graphics in communicating a consumer’s choice over how websites can use their personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020); Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020).		
12.	The button should not be mandatory because it is impractical and infeasible in a variety of contexts where the link might reasonably be presented (e.g., in a bullet-pointed list in a sidebar menu, in the footer of an email message, or in the app download page of the app store). It would also exacerbate the problem with fitting the link’s required text into space-restricted contexts, such as in a mobile app, etc.	No change has been made in response to this comment. Use of the icon is optional. The OAG developed the icon to provide an opportunity for businesses to promote consumer awareness of their privacy rights under the CCPA. If a business wants to promote a consumer’s privacy rights by using the icon, the regulation requires the icon to be placed to the left of the “Do Not Sell My Personal Information” link. This location is mandatory because it promotes awareness of the consumer’s right to opt out of the sale of their personal information. Businesses may use the icon in additional locations at their discretion. This is in order to facilitate multiple pathways for the consumer to exercise their right to opt-out. See Habib, et al., “It’s a scavenger hunt”: Usability of Websites’ Opt-Out and Data Deletion Choices, CHI ’20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, April 2020, Honolulu, HI, USA, at pg. 7.	W397-5 W400-3	00001-00002 00026
13.	The button should not be mandatory because it would create additional work for businesses that have already made a good-faith effort to comply with the regulatory requirements.	No change has been made in response to this comment. Civil Code § 1798.185(a)(4)(C) requires the OAG to develop a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information. Use of the icon is optional. The OAG developed the icon to provide an opportunity for businesses to promote consumer	W397-6 W401-3	00002 00032

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
		<p>awareness of their privacy rights under the CCOA. If a business promotes a consumer’s privacy rights by using the icon, the regulation requires the icon to be placed to the left of the “Do Not Sell My Personal Information” link. This location is mandatory because it promotes awareness of the consumer’s right to opt out of the sale of their personal information. Businesses may use the icon in additional locations at their discretion. The OAG selected the blue toggle design after testing a number of different graphics with consumers and finding that the blue toggle design performed much better than the other graphics in communicating a consumer’s choice over how websites can use their personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020); Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020). To the extent that the regulations require incremental compliance, the OAG may exercise prosecutorial discretion if warranted, depending on the particular facts at issue. Prosecutorial discretion permits the OAG to choose which entities to prosecute, whether to prosecute, and when to prosecute. Moreover, Civil Code § 1798.155(b) provides businesses with 30 days to cure any alleged noncompliance.</p>		
14.	<p>The button design is impractical and may be confusing to consumers because it appears to be a toggle button. It is not a choice for opting in or out but a repetitive link that is redundant and may cause consumers to overlook the link itself, or think it is for opting-in to the sale of personal information.</p>	<p>No change has been made in response to this comment. The OAG selected the blue toggle design after studying and testing a number of different graphics with consumers and finding that the blue toggle design performed much better than the other graphics in communicating a consumer’s choice over how websites can use their personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020); Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020). Cranor’s study addressed its design, noting that it selected one color (blue) to avoid conveying a particular state, such as green and red (which are commonly used in actual toggles). See Cranor, et al., (February 4, 2020) at p. 11. Furthermore, when engaged in user testing, the misconception that the toggle was viewed as an actual control was</p>	<p>W400-4 W402-6 W403-2 W405-2</p>	<p>00026 00040 00042 00052-00053</p>

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
		rare (6 of 1,416 respondents in total, or less than 0.5%). See Cranor, et al., (February 4, 2020) at p. 31. As corroborated in Cranor’s study and as explained in the second addendum to the FSOR, the icon is to be used with the “Do Not Sell My Personal Information” link to build awareness for its meaning. The comment offers no alternative design that would be more effective or as effective and less burdensome than the icon selected by the OAG.		
15.	The requirement in (f)(3) that the opt-out button be the same size as other buttons is confusing because button sizes are often inconsistent across different pages and websites, etc. It is unclear whether the button should be the same size as other buttons on the particular page or across multiple pages of a website.	No change has been made in response to this comment. The regulation is reasonably clear and the OAG does not believe additional guidance to the level of detail the comment is seeking is necessary. Section 999.306(f)(3) states that the icon shall be approximately the same size as other icons used by the business on its webpage. No other comments have raised similar concerns. Businesses should use their discretion in applying this regulation.	W400-5	00026-00027
16.	The recent passage of Proposition 24 – the CA Privacy Rights Act (CPRA) requires a rulemaking which will establish a process to select an effective icon. This requisite renders a robust stakeholder process to identify the merits of any particular icon and the efficacy by which it will develop a concise, usable instrument. Identifying an icon would circumvent the process just after one was approved by the voters. The icon development process should go through the CPRA route in the CA Privacy Protection Agency.	No change has been made in response to this comment. The CPRA does not amend any of the statutory language regarding the opt-out logo or button. See Civ. Code, § 1798.185(a)(4)(C). The OAG developed the icon to provide an opportunity for businesses to promote consumer awareness of their privacy rights under the CCPA. If a business promotes a consumer’s privacy rights by using the icon, the regulation requires the icon to be placed to the left of the “Do Not Sell My Personal Information” link. This location is mandatory because it promotes awareness of the consumer’s right to opt out of the sale of their personal information. Businesses may use the icon in additional locations at their discretion. The OAG has solicited broad public participation in the adoption of regulations, including those pertaining to the opt-out icon, and selected the blue toggle design after studying and testing a number of different graphics with consumers and finding that the blue toggle design performed much better than the other graphics in communicating a consumer’s choice over how websites can use their personal information. See Cranor, et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale	W402-4 W412-3	00040 00086-00088

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
		of Personal Information as Required by CCPA (February 4, 2020); Cranor, et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020).		
17.	The opt-out button only pertains to the opt-out of sale when the notice at collection and notice of financial incentive are equally foundational elements of CCPA notice transparency. Consumers may misunderstand and misuse the opt-out button to be used for any privacy purpose. CA should instead adopt a Nutrition Label-style framework as a foundational tool for meeting the notice transparency requirements of CCPA/CPRA. A Privacy Facts label would display simple and concise privacy information in real time as directed by the consumer. It provides an operational means for transitioning away from the misuse of cookie notices and banners.	No change has been made in response to this comment. The proposed modification to § 999.306 does not pertain to a business’s obligation to provide a notice at collection or a notice of financial incentive. Sections 999.305 and 999.307 pertain to those notices and are already in effect. Civil Code § 1798.185(a)(4)(C) requires the OAG to develop a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information, not a button for any privacy purpose. In drafting these regulations, the OAG has considered the wide variety of different industries subject to the CCPA, as well as the costs to be incurred by the various businesses in complying with the law. For the reasons set forth in the ISOR, FSOR, and the second addendum to the FSOR, the OAG determined that the current framework implements the CCPA in a manner that provides flexibility and is cost effective and less burdensome on businesses. The comment’s proposed change to implement a mandatory nutrition label-style framework may not best address all the different factual situations and industries in which the CCPA requires disclosures at this time. However, the OAG appreciates the comment and continues to observe business trends and best practices as part of its ongoing rulemaking authority.	W407-1	00063-00066
18.	The opt-out mechanism is problematic on multiple fronts: (1) It only applies to the “sale” of user data and not to sharing of user data, even though portable data can be shared with a service provider, who could sell the data without any notice or consent. (2) It places the burden on the individual to, in essence, opt-in to privacy, which fails to align with the human right of privacy; it also fails the principle of privacy as the default setting in Privacy by Design. (3) It presents significant difficulty in developing a global privacy signal standard, as	No change has been made in response to this comment. The comment objects to the CCPA, not the proposed regulation. Civil Code § 1798.120 gives consumers the right to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information. It provides an opt-out framework, not an opt-in to the sale of personal information (except when it comes to the personal information of consumers under the age of 16). Also, Civil Code § 1798.140(t)(2)(C) specifically states that information shared with a service provider (as defined by Civil Code § 1798.140(v)) does not constitute a “sale.” Contrary to the comment’s statement, a service provider may not sell the data without notice. To do so would take them out of the definition of “service	W410-1	00076-00080

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
	the European Union in recent decisions has made clear that opt-out is not GDPR-compliant. (4) Opting-Out presents a particularly confusing user interface (UI) in communicating a negative/opt-out.	provider.” The OAG cannot implement regulations that alter or amend a statute or enlarge or impair its scope.		
General Comment Regarding All Modifications				
19.	Adding new requirements makes compliance more difficult for businesses and impacts consumers’ ability to exercise their CCPA rights. The AG should stop rulemaking for a while to allow businesses to implement the current regulations and to allow regulators to identify true challenges to the new rules.	No change has been made in response to this comment. The OAG disagrees with the comment. In drafting these regulations, the OAG has considered the burden on businesses as well as consumers’ ability to exercise their CCPA rights. As set forth in the 2nd Addendum to the FSOR, the proposed regulations provide guidance to businesses and bring clarity where there may have been some ambiguity. They also address real barriers consumers face when exercising their CCPA rights.	W400-1	00025
20.	The modifications should include language making the changes effective six months to one year from publication of final regulations to give businesses time to implement them. This time is especially important during the ongoing COVID-19 crisis where personnel are working remotely and businesses are continuing to recover from being shut down.	No change has been made in response to this comment. The OAG has considered and determined that delaying the implementation of these regulations is not more effective in carrying out the purpose and intent of the CCPA. The proposed modifications are minimal and many were introduced earlier on in the rulemaking process. Thus, businesses have been aware that these requirements could be imposed as part of the OAG’s regulations. To the extent that the regulations require incremental compliance, the OAG may exercise prosecutorial discretion if warranted, depending on the particular facts at issue. Prosecutorial discretion permits the OAG to choose which entities to prosecute, whether to prosecute, and when to prosecute. Moreover, Civil Code § 1798.155(b) provides businesses with 30 days to cure any alleged noncompliance. Thus, any regulation that delays implementation of the regulations is not necessary.	W402-2 W409-3	00039 00073
21.	The proposed amendments are unlawful and invalid because they violate the California APA; the Attorney General must withdraw them and restart a new notice period. Government Code section 11346.4(b) states that a Notice of Proposed Action is valid for one year, and these proposed amendments were published 367	No change has been made in response to this comment. The proposed modifications to the regulations do not violate the California Administrative Procedures Act. The Governor’s Executive Orders N-40-20 and N-66-20 extended the deadline to complete and transmit a rulemaking package to the Office of Administrative Law (OAL) by 120 calendar days.	W408-3	00070

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
	days after the original Notice of Proposed Action.	Accordingly, the OAG has until February 7, 2021 to complete and submit its rulemaking package to OAL.		
COMMENTS NOT DIRECTED AT 15-DAY MODIFIED TEXT				
22.	The AG should remove § 999.315(h)(1) and (h)(5) or add qualifying language that it not be done “to an excess or unreasonable degree.”	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. The modifications do not affect § 999.315(h).	W397-7	00002-00003
23.	Illustrative examples set forth in § 999.315(h)(1)-(5) should not use the language “shall not.” Regulation should adopt a reasonableness standard instead.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. The modifications do not affect § 999.315(h).	W400-6	00027-00028
24.	Section 999.315(h)(3) limits businesses’ ability to provide more transparency to consumers and raises compelled speech issues.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. The modifications do not affect § 999.315(h).	W400-6 W401-4	00027-00028 00032-00035
25.	The AG should clarify in § 999.315 that offers to customers are allowed if the display of such offers adds no additional steps to the opt-out process.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. The modifications do not affect § 999.315(h).	W406-2	00058-00059
26.	A business should be allowed to both verify a consumer’s identity and to confirm that the consumer provided the authorized agent permission to submit the request on his/her behalf in order to prevent identify theft. Also, businesses should be allowed to require authorized agents to verify their own identities. Otherwise, fraudsters could pose as authorized agents to access consumers’ personal information.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. Similar comments are addressed in Appendix G, responses 36 and 37.	W402-3 W405-3 W406-3 W408-2 W409-2 W412-2	00039-00040 00053-00055 00059-00060 00069-00070 00073 00086-00087
27.	The AG should clarify that if an authorized agent inadvertently submits a request incorrectly, the company must either accept it or inform the agent how to submit it appropriately.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W398-3	00009

FSOR APPENDIX I: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING FOURTH 15-DAY COMMENT PERIOD

Response #	Summary of Comment	Response	Comment #s	Bates Label (CCPA_4TH15DAY_)
28.	The AG should impose the same notice requirements imposed on businesses on authorized agents.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. Similar comments are addressed in Appendix G, response 38.	W401-5	00035
29.	The AG should clarify the definition of sale and tighten the restrictions on service providers to ensure that consumers can opt out of cross-context targeted advertising.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W398-4	00009-00010
30.	The AG should use its rulemaking authority to close gaps or to exercise his prosecutorial discretion to put industry on notice that they are not liable for business practices that will be lawful when CPRA goes into effect in 2023; specifically with regard to information in the public domain and honoring user-enabled global privacy controls.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period.	W404-2	00045-00047
31.	Comment attaches commenter’s previously submitted comments to the 3rd set of proposed modifications.	No change has been made in response to this comment. The comments do not relate to any modification to the text for this 15-day comment period. Responses to commenter’s previously submitted comments are addressed in Appendix G, responses 7, 9, 30, 42, 43, and 44.	W398-5	00011-00021

FSOR APPENDIX J: LIST OF COMMENTERS FROM 4TH 15 DAY PERIOD

Name	Organization	Comment #	Response #
Anonymous		W397-1	1
		W397-2	6
		W397-3	8
		W397-4	9
		W397-5	12
		W397-6	13
		W397-7	22
Maureen Mahoney	Consumer Reports	W398-1	5
		W398-2	9
		W398-3	27
		W398-4	29
		W398-5	31
Steven K. Hazen		W399-1	9
Dylan Hoffman	Internet Association	W400-1	19
		W400-2	9
		W400-3	12
		W400-4	14
		W400-5	15
		W400-6	23, 24
Mike Signorelli, Allie Monticollo, Dan	Venable, LLP;	W401-1	9
Jaffe, Christopher	Association of National Advertisers, American	W401-2	10
Oswald, David LeDuc,	Association of	W401-3	13
Lou Mastria, Alison	Advertising Agencies,	W401-4	24
Pepper, David	IAB, American	W401-5	28
Grimaldi, Clark Rector	Advertising Federation, DAA, Network Advertising Initiative	W401-6	2
Cameron Demetre	Technet	W402-1	1
		W402-2	20
		W402-3	26
		W402-4	16

Name	Organization	Comment #	Response #
Stephanie Lucas		W402-5	9
		W402-6	14
		W403-1	7
Sara DePaul, Christopher A. Mohr	Software & Information Industry Association	W403-2	14
		W403-3	8
		W404-1	11
Melanie Tiano, Gerard Keegan	CTIA	W404-2	30
		W405-1	9
		W405-2	14
Emily Emery, Brigitte Schmidt Gwyn, Rita Cohen	The Association of Magazine Media	W405-3	26
		W406-1	3
		W406-2	25
Dale Smith	PrivacyCheq	W406-3	26
Shoeb Mohammed	CalChamber	W407-1	17
		W408-1	9
		W408-2	26
Jesse Vallejo, Kyla Christoffersen Powell	Civil Justice Association of California	W408-3	21
		W409-1	9
		W409-2	26
Lisa LeVasseur	Me2B Alliance	W409-3	20
		W410-1	18
Jake Snow	ACLU of Northern California, Common Sense Kids Action, EFF, Privacy Rights Clearinghouse	W410-2	4
		W411-1	5
Jim Halpert	State Privacy & Security Coalition	W412-1	1
		W412-2	26
		W412-3	16
		W412-4	9