

Message

From: K. Stout [REDACTED]
Sent: 12/6/2019 9:07:26 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Alec Stapp [REDACTED]; Julian Morris [REDACTED]
Subject: ICLE Comments on CCPA Rulemaking Proceeding
Attachments: ICLE - CCPA Implementation Comments-final.pdf

Dear Privacy Regulations Coordinator,

Please find attached the comments of the International Center for Law & Economics on the pending rule making process for the California Consumer Privacy Act regulations currently being undertaken by the Office of the Attorney General. Please feel free to reach out to us with any comments or questions.

Thank you,

Kristian Stout
Associate Director | International Center for Law & Economics

[REDACTED]
[@kristianstout](#)
laweconcenter.org | truthonthemarket.com



Comments on the California Consumer Privacy Act (CCPA)

International Center for Law & Economics

Authored By:

Kristian Stout, Associate Director

Alec Stapp, Research Fellow

Before the

**STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL**

Sacramento, CA 94244

In the Matter of the California Consumer Privacy Act (CCPA)

**COMMENTS OF THE INTERNATIONAL CENTER FOR LAW &
ECONOMICS**

December 6, 2019

Executive Summary

We thank the Attorney General’s Office (“AG’s Office”) for the opportunity to comment on this timely and highly relevant policy discussion. We begin our analysis of the California Consumer Privacy Act (“CCPA”) with a discussion of the standardized regulatory impact assessment (SRIA) prepared for the AG’s Office by Berkeley Economic Advising and Research, LLC.¹ The bottom-line cost figures from this report are staggering: \$55 billion in upfront costs and \$16.5 billion in additional costs over the next decade.² The analysis includes large benefits as well, but as we will show below, the actual costs are even higher than the SRIA estimates and the benefits fall far short of making up for those costs.

Related, the AG’s Office should take note of some of the early evidence of how the EU’s General Data Protection Regulation (“GDPR”) is faring.³ After its first twelve month period in force, the compliance costs were astronomical; enforcement of individual “data rights” led to unintended consequences; “privacy protection” seems to have undermined market competition; and there have been large unseen – but not unmeasurable – costs in forgone startup investment.⁴

In one example of the ultimate scale of the compliance costs, Google reportedly spent “hundreds of years of human time” in order to be compliant with GDPR.⁵ Nonetheless, France still found it noncompliant, levying a \$57 million fine against the company for noncompliance.⁶ A report by the Internet Association of Privacy Professionals estimated that roughly 500,000 firms in the EU registered a data protection officer.⁷ Data protection officers can serve more than one organization, but the number of actual officers is undoubtedly large, and at an average salary of \$88,000,⁸ amount to a huge ongoing cost.

Consider this in the context of the SRIA’s findings. The SRIA provides a very rough estimate of affected businesses based on assumptions about revenue per employee in order to arrive at a range

¹ Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, August 2019, http://www.dof.ca.gov/Forecasting/Economic/Major_Regulations/Major_Regulations_Table/documents/CCPA_RegulationsSRIA.DOE.pdf [hereinafter SRIA].

² *Id.*

³ See, e.g., Alec Stapp, *GDPR After One Year: Costs and Unintended Consequences*, TRUTH ON THE MARKET, May 24, 2019, <https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/>.

⁴ *Id.*

⁵ Ashley Rodriguez, *Google Says It Spent “Hundreds of Years of Human Time” Complying With Europe’s Privacy Rules*, QUARTZ, Sep. 26, 2018, <https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr/>.

⁶ Tony Romm, *France Fines Google Nearly \$57 Million for First Major Violation of New European Privacy Regime*, WASHINGTON POST, Jan. 21, 2019, https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.

⁷ *Approaching One Year GDPR Anniversary, IAPP Reports Estimated 500,000 Organizations Registered DPOs in Europe*, Internet Association of Privacy Professionals, May 16, 2019, <https://iapp.org/about/approaching-one-year-gdpr-anniversary-iapp-reports-estimated-500000-organizations-registered-dpos-in-europe/>.

⁸ *Id.*

of between 9,858 and 570,066 affected businesses.⁹ Already this rough estimate exceeds the number of firms that registered data protection officers in the EU, but the SRIA further opines that “[a] lack of data prevents us from estimating with precision the number of businesses that meet the other threshold requirements in the CCPA”¹⁰ – suggesting that the actual compliance costs of all affected firms could be significantly higher. And this is just for firms within California, leaving aside the compliance costs to extraterritorial firms that reach the statutory thresholds for California customers or users.

Implementation of GDPR also led to a host of unintended consequences. Although GDPR was designed to reign in the power of large ad-tech companies, like Google and Facebook, it perversely resulted in smaller vendors suffering more harm than the large companies.¹¹ Venture funding also appears to have taken a hit, with a “17.6% reduction in the number of weekly venture deals, and a 39.6% decrease in the amount raised in an average deal following the rollout of GDPR.”¹² And it is the latter sort of unintended consequence that should be most troubling to regulators, as all too often there do not even exist proxies like VC funding by which to judge the pro-social behavior (like starting new companies) that laws like GDPR and the CCPA silently deter.

Finally, despite the DC Circuit trimming the FCC’s 2018 Restoring Internet Freedom Order (“RIF Order”),¹³ the fact remains that the FCC still retains a conflict-preemption authority to specifically preempt state laws that are incompatible with its regulations.¹⁴ To wit,

Conflict preemption applies to “state law that under the circumstances of the particular case stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress—whether that ‘obstacle’ goes by the name of conflicting; contrary to; repugnance; difference; irreconcilability; inconsistency; violation; curtailment; interference, or the like.”¹⁵

The DC Circuit only limited the FCC’s ability to *generally* preempt all potentially conflicting state laws, requiring that each preemption be challenged in a fact-intensive inquiry.¹⁶

⁹ See SRIA, *supra*, note 1, pp. 20-21 and Table 2.

¹⁰ *Id.* at 20.

¹¹ See, e.g., Greg Ip, *Beware the Big Tech Backlash*, WALL STREET JOURNAL, Dec. 19, 2018, <https://www.wsj.com/articles/beware-the-big-tech-backlash-11545227197>; see also Jessica Davies, ‘The Google Data Protection Regulation’: GDPR is Strafing Ad Sellers, DIGIDAY, June 4, 2018, <https://digiday.com/media/google-data-protection-regulation-gdpr-strafting-ad-sellers/>.

¹² Jian Jia, Ginger Zhe Jin, and Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment*, NBER Working Paper No. 25248 (2018) available at <https://www.nber.org/papers/w25248>

¹³ *Mozilla Corp. v. Fed. Commc'ns Comm'n*, 940 F.3d 1, 18 (D.C. Cir. 2019).

¹⁴ *Id.* at 81.

¹⁵ *Id.*

¹⁶ *Id.*

Similarly, it is also possible that the broad extent of the CCPA's rules, and their impositions on firms outside of California's borders could lead to Dormant Commerce Clause challenges.¹⁷ Activities that "inherently require a uniform system of regulation" or that "impair the free flow of materials and products across state borders" violate the Dormant Commerce Clause.¹⁸ As the FCC noted in its RIF Order, Internet-based communications is such a type of activity.¹⁹

Recommendations

The AG's Office should take great care in implementing the CCPA as both the known and the unknown costs are very large, and the law, if incorrectly implemented, will be subject to serious federal challenge. There are a handful of modifications that we believe may help navigate these shoals. Each suggestion is discussed in more depth, *infra*.

- 1- Clarify the definition of "personal information" so that it is not overinclusive of incidental information and also does not allow third-parties to claim rights over others' data;
- 2- Stress that the "valuation" of data is a difficult exercise, and the requirements to value data when offering different tiers of service shall be interpreted liberally;
- 3- Clarify that the definition of a "business" does not mean that *any* firm that "receives for the business's commercial purposes" an individual's personal information includes firms that merely "receive" information on consumers as a normal part of operations. For example, a website that logs a user's behavior through its site "receives" location, IP Address, and other information about that user, but *should not* be included in such a broad definition;
- 4- Delay implementation until there is a broadly available means of ensuring that firms can reliably ascertain the validity of user data requests (i.e. that, as is happening under the GDPR, third-parties are not able to obtain information on the customers of firms by representing themselves as those customers); and
- 5- Use the authority granted by the CCPA to establish a necessary exception in order to comply with applicable federal law to temporarily delay implementation until (1) it is determined that the law does not violate the Dormant Commerce Clause, and (2) the AG's Office has the opportunity to consult with the FCC and ensure that the CCPA is not subject to conflict-preemption in light of the FCC's authority over Internet communications.

¹⁷ See, e.g., Jennifer Huddleston and Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations*, Regulatory Transparency Project (2019) available at <https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf>; see also Graham Owens, *Federal Preemption, the Dormant Commerce Clause, and State Regulation of Broadband: Why State Attempts to Impose Net Neutrality Obligations on Internet Service Providers Will Likely Fail*, TechFreedom (2018) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216665. Better cite: <https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf>

¹⁸ Ark. Elect. Co-op. Corp. v. Arkansas Pub. Serv. Comm'n, 461 U.S. 375, 384 (1984).

¹⁹ *In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, FCC 17-166 (Jan. 4, 2018) available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0104/FCC-17-166A1.pdf [hereinafter RIF Order].

I. The SRIA analysis shows costs exceeding benefits

To start, there is a lot of uncertainty in estimating the benefits of privacy regulations to consumers, as well as the costs of compliance. Among other things, no one actually knows how many businesses the CCPA will cover, even though it will go into effect in less than a month. Indeed, the SRIA estimates that somewhere between 9,858 and 570,066 California businesses will be covered by the new law.²⁰ That is, to say the least, quite a margin of error. Such uncertainty inevitably chills business activity and can even pose rule of law issues (e.g., a conscientious entrepreneur may reasonably believe their business falls outside the scope of the CCPA when in fact it does not).

As Daniel Castro and Alan McQuinn point out, these higher estimates arise because, in addition to gross annual revenue thresholds, “businesses with websites that receive traffic from an average of 137 unique Californian IP addresses per day could be subject to the new rules.”²¹ Even the Notice of Proposed Rulemaking Action (“NPRMA”) in this matter demonstrates the ambiguity in the law. In its summary of the law, the NPRMA describes one of the categories of businesses subject to CCPA requirements as those that “[b]uy[, receive[, or sell] the personal information of 50,000 or more consumers, households, or devices[.]”²² And, according to the text of the law, the statute applies to any firm that

Alone or in combination, annually **buys, receives** for the business’s commercial purposes, **sells, or shares** for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.²³

Yet, later in the NPRMA, the same class of businesses is described as “businesses that **buy, sell, or share** the personal information of more than 50,000 consumers, households, or devices per year[.]”²⁴

It may seem a minor distinction, but the difference between a business that merely “receives” consumer information and one that “buys,” “sells,” or “shares” consumer information is *very* different and goes back to Castro and McQuinn’s point. A website that passively logs information on all of its visitors for completely innocuous purposes certainly “receives” information on consumers. But this is very different than a website that actively scrapes user information, purchases it for integration with data sets, or sells large amounts of consumer data as part of its regular course of business. Yet, under the highly ambiguous definitions in the law, these behaviors are treated equally.

²⁰ SRIA, *supra*, note 1 at 22.

²¹ Daniel Castro and Alan McQuinn, *Comments on the California Consumer Privacy Act, Assembly Bill 375, Rulemaking Process*, Information Technology & Innovation Foundation 4, Mar. 8, 2019, available at <http://www2.itif.org/2019-comments-ccpa.pdf>

²² Notice of Proposed Rulemaking Action, California Department of Justice, 3 (Oct. 11, 2019) available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf> (emphasis added) [hereinafter NPRMA].

²³ California Consumer Privacy Act, California Civil Code § 1798.140(c)(1)(B).

²⁴ *Id.* (emphasis added)

Notably, the SRIA uses the conservative, low end of its range for its “baseline” estimates. But the report also includes estimates for scenarios in which up to thirty times more companies are covered than in the conservative baseline. For reference, according to a survey by the International Association of Privacy Professionals (“IAPP”), 79 percent of respondents believe their employer must comply with the CCPA, so the higher end of the range is likely closer to reality than the lower end.²⁵ Also, it must be noted, the report looks at only the incremental effects of the CCPA. So, all of these costs are in addition to – not in lieu of – the costs companies already incur to comply with privacy rules.

A. Direct Costs

According to the SRIA, the CCPA will impose on California businesses approximately \$55 billion in initial compliance costs, or 1.8 percent of California’s 2018 Gross State Product (GSP):

Assume that smaller firms (<20 employees) will incur \$50,000 in initial costs (the median of the lowest cost category), medium-sized firms (20-100 employees) incur an initial cost of \$100,000 (the maximum of the lowest cost category in the survey), medium/large firms (100-500 employees) incur an initial cost of \$450,000, and firms with greater than 500 employees incur, on average an initial cost of \$2 million. Also assume that 75% of all California businesses will be required to comply with the CCPA (see Section 2.1 for detailed estimates of the number of firms affected by firm size and industry). The total cost of initial compliance with the CCPA, which constitutes the vast majority of compliance efforts, is approximately \$55 billion. This is equivalent to approximately 1.8% of California Gross State Product in 2018.²⁶

In addition, the CCPA will impose on California businesses up to another \$16.45 billion in costs over the next decade, as this table from the SRIA shows:

²⁵ *Ready or Not, Here It Comes: How Prepared are Organizations for The California Consumer Privacy Act?*, Internet Association of Privacy Professionals, 8 (2019) available at https://www.onetrust.com/wp-content/uploads/2019/04/onetrust-iapp_ccpa-benchmarkingreport.pdf.

²⁶ SRIA, *supra*, note 1 at 11.

Table 3: Total Estimated Compliance Costs (million 2019\$)

NAICS Code	Description	>\$25 million revenue threshold	50% Threshold	75% Threshold
11				40.5
21	Mining, Quarrying, and Oil and Gas Extraction	2.1	9.0	12.6
22	Utilities	1.4	8.3	11.8
23	Construction	16.9	1,026.8	1,536.1
31-33	Manufacturing	48.1	530.8	780.7
42	Wholesale Trade	49.5	755.3	1,116.5
44-45	Retail Trade	32.2	1,021.3	1,522.0
48-49	Transportation & Warehousing	25.0	293.8	431.3
51	Information	20.3	248.1	365.1
52	Finance and Insurance	24.6	429.0	634.3
53	Real Estate, Rental, Leasing	13.8	624.2	931.6
54	Professional, Scientific, and Technical Services	51.6	1,686.0	2,511.6
55	Management of Companies and Enterprises	46.2	65.2	80.0
56	Administrative/Support/Waste Mgmt. Svs.	33.5	551.9	816.9
61	Educational Services	12.2	184.5	273.7
62	Health Care and Social Assistance	34.5	1,329.6	1,986.0
71	Arts, Entertainment, and Recreation	8.3	340.7	508.7
72	Accommodation and Food Services	29.2	953.0	1,422.4
81	Other Services (except Public Administration)	16.4	984.8	1,472.5
Total		466.9	11,069.4	16,454.2

While these cost estimates are indeed significant, there remains one major problem with the SRIA analysis. As the report itself notes, none of these estimates includes the costs incurred by the hundreds of thousands of companies outside of California to which the regulation applies:

The SRIA requires an analysis of the impact of proposed major regulations on California businesses. However, the CCPA will also affect businesses that provide goods and services to California consumers. There are likely to be many businesses that are not located in California (and therefore not captured in SUSB statistics) but serve California customers. The economic impact of the regulations on these businesses located outside of California is beyond the scope of the SRIA and therefore not estimated.²⁷

Interestingly, an independent analysis by IAPP estimated that 507,280 businesses (including those outside of California) would be liable under the CCPA – about the same as the report’s high-end, California-only number.²⁸ The reality is likely higher given IAPP’s conservative calculations. And, of course, neither of these estimates counts non-US firms. Most importantly, the foregoing includes only *direct* costs; there are large *indirect* costs as well that need to be taken into account.

²⁷ *Id.* at 21.

²⁸ Rita Heimes and Sam Pfeifle, *New California Privacy Law to Affect More Than Half A Million US Companies*, Internet Association of Privacy Professionals, Jul. 2, 2018, available at <https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/>

B. Indirect Costs

The SRIA points to GDPR compliance for reference, noting that, in addition to a substantial increase in IT budgets, the GDPR has also likely led to reduced productivity:

Collectively, these costs represent a 1640% increase in annual IT budgets (Christensen et al 2013). In addition to compliance costs, there is also evidence that the GDPR's stricter data policies have reduced firm productivity in sectors that rely heavily on data (Ferracane et al 2019) with the biggest impacts found in firms devoted to data profiling (Cave et al 2012).²⁹

The report provides some estimates of the CCPA's likely macroeconomic effects but dismisses them as "completely negligible in relation to the economy as a whole."³⁰ But are they really negligible? Here is the relevant table from the SRIA:³¹

Table 6: Economy-Wide Impacts of CCPA Regulations
(billion\$ differences from baseline, 2015 dollars unless otherwise noted)

	\$25 Million Revenue Threshold		
			2030
Real GSP	-0.070	-0.110	-0.140
Employment (1,000 FTE)	-0.180	-0.310	-0.430
Real Output	-0.070	-0.120	-0.170
Investment	-0.030	-0.030	-0.040
Household Income	-0.040	-0.060	-0.080
	50% Threshold		
			2030
Real GSP	-1.680	-2.380	-3.090
Employment (1,000 FTE)	-4.550	-7.190	-9.520
Real Output	-1.560	-2.630	-3.740
Investment	-0.590	-0.690	-0.770
Household Income	-0.890	-1.310	-1.750
	75% Threshold		
			2030
Real GSP	-2.500	-3.530	-4.600
Employment (1,000 FTE)	-6.770	-10.690	-14.150
Real Output	-2.320	-3.900	-5.560
Investment	-0.880	-1.030	-1.140
Household Income	-1.320	-1.950	-2.610

This table shows that, over the next ten years, the CCPA could result in a loss of \$4.6 billion in gross state product (GSP), 14,000 jobs, and \$9.3 billion in output, investment, and income. Given California's size, these estimates are small on a relative basis but large on an absolute basis. And, in

²⁹ SRIA, *supra*, note 1 at 12.

³⁰ *Id.* at 39.

³¹ *Id.*

comparison to the low value consumers place on privacy,³² the costs to productivity and employment are unacceptably high.

The SRIA also does not count the higher costs of advertising and lost advertising revenue. A compelling estimate by Catherine Tucker, a professor of marketing at the Massachusetts Institute of Technology, and Avi Goldfarb, a professor of marketing at the University of Toronto – based on their research on the effects of EU privacy regulations on advertising effectiveness – suggests this cost is also well into the billions of dollars:³³

[S]eeing one plain banner ad increases purchase intent by 2.63 percentage points. The introduction of privacy laws in the EU was associated with a decrease in this effectiveness of 1.71 percentage points, or around 65%. **Therefore, for an advertiser to achieve the same lift in likely intent as they did prior to the law, they would have to buy 2.85 times as much advertising.**

Currently in the United States, \$8 billion is spent per year on the type of display-related advertising that we study (Interactive Advertising Bureau (IAB) 2010). If prices and demand of advertising did not change, that would mean that advertisers would have to spend \$14.8 billion more than they are currently doing to achieve the same increase in purchase intent after the introduction of privacy regulation.³⁴

This is a positive result for the incumbent advertising platforms, which have the resources necessary for compliance and the direct relationship with end users necessary to secure consent. As Antonio García Martínez wrote recently,

Facebook and Google ultimately are not constrained as much by regulation as by users. **The first-party relationship with users that allows these companies relative freedom under privacy laws comes with the burden of keeping those users engaged and returning to the app,** despite privacy concerns.³⁵

The benefits to dominant advertising platforms come at a high cost to consumers and advertisers. Moreover, this kind of differential impact is anathema to the goals of public policy. Regulatory benefits accruing to particular firms – at the expense of consumers – are anti-competitive in nature and

³² See discussion, *infra*, at notes 45 -55 and accompanying text; see also Will Rinehart, *Hearing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation*, American Action Forum, Oct. 24, 2019, available at <https://www.americanactionforum.org/testimony/hearing-on-data-ownership-exploring-implications-for-data-privacy-rights-and-data-valuation/>

³³ N.B., further data is needed to reach a more precise estimate.

³⁴ Avi Goldfarb and Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 1 *MANAGEMENT SCIENCE* 57, 68, available at <https://pdfs.semanticscholar.org/41dd/8ac2799fbeeac0d13e0af3a16d994a2dcd928.pdf> (emphasis added)

³⁵ Antonio García Martínez, *Why California's Privacy Law Won't Hurt Facebook or Google*, *WIRED*, Aug. 31, 2018, <https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/> (emphasis added)

can become self-reinforcing, biasing market competition in favor of incumbents and against new entrants.

C. Benefits

First, researchers still debate the degree to which consumers actually value privacy, so assessing the benefits under the CCPA is difficult. The bulk of the empirical research on the economics of privacy shows that, while consumers' privacy valuations are highly context-dependent, they tend to be extremely low and often pale in comparison to other considerations such as cost and convenience.³⁶

Furthermore, the measurement problems with this endeavor are significant, with the SRIA even acknowledging the extreme uncertainty of any estimates of the regulation's benefits. Nevertheless, it offers a couple of possible measures for benefits: \$1.6 to \$5.4 billion based on consumers' willingness to pay ("WTP") for more app privacy; \$169 million based on the implied value of firms' WTP for consumers' basic information; \$9.7 billion based on the implied value of firms' WTP for more-sensitive information; and \$12 billion based on the average revenue per user ("ARPU") of personal information used for advertising in California.

Despite the report's assumption to the contrary, other than the first of these, none of these metrics estimates the value *to consumers* of increased privacy regulation. Rather, they estimate the value *to firms* of the underlying data. In no sense does the CCPA somehow transfer this value to consumers. Some of the CCPA's costliest rules require disclosure, but this does not inherently preserve value. It might trigger additional expense to claw data back, but it does not simply confer its value on consumers.

Indeed, much of the value of this data – and presumably all of its value to businesses – arises from its use by businesses. Therefore, keeping it out of firms' hands does not transfer that value to consumers – it *destroys* that value. The CCPA's opt-out rules will impede firms' ability to offer targeted ads and publishers' ability to finance content with advertising. This limitation will likely lead to significant consumer costs, including higher product prices, less information flow, and subscription fees.³⁷

All of these issues are ignored by the SRIA.

Based on the report's one arguably valid measure of the regulation's benefits (i.e., consumer WTP for more privacy), the CCPA would confer between \$1.6 to \$5.4 billion per year in benefits at a cost – including both annualized up-front costs and ongoing costs over ten years – of \$7.2 billion per year. Even ignoring the problems with these estimates, this is a poor outcome for California consumers.

³⁶ See, *infra*, at notes 38– 55 and accompanying text.

³⁷ See generally Avi Goldfarb and Catherine E. Tucker, *supra*, note 34.

II. The economics of valuing user data

Under § 1798.125, businesses are permitted to discriminate between consumers that allow data collection and those who choose to opt-out.³⁸ There is an important proviso, however. Nothing in the CCPA, “prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, **if that difference is reasonably related to the value provided to the consumer by the consumer’s data.**”³⁹

The manner in which the AG’s Office plans to interpret this rule is potentially problematic and requires careful consideration of the economics of user data. The AG’s Office proposes to require the following pursuant to § 1798.125:

To estimate the value of the consumer’s data, a business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer’s data. The business shall use one or more of the following:

- (1) The marginal value to the business of the sale, collection, or deletion of a consumer’s data or a typical consumer’s data;
- (2) The average value to the business of the sale, collection, or deletion of a consumer’s data or a typical consumer’s data;
- (3) Revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value;
- (4) Revenue generated by the business from sale, collection, or retention of consumers’ personal information;
- (5) Expenses related to the sale, collection, or retention of consumers’ personal information;
- (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference;
- (7) Profit generated by the business from sale, collection, or retention of consumers’ personal information; and
- (8) Any other practical and reliable method of calculation used in good-faith.⁴⁰

³⁸ California Civil Code 1798.125 (a)(2).

³⁹ *Id.* (emphasis added).

⁴⁰ Proposed California Consumer Privacy Act Regulations § 999.337. Calculating the Value of Consumer Data, *available at* <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>.

There are, broadly speaking, two classes of “calculation” this rule contemplates: one performed by firms that explicitly traffic in data as a commodity (e.g. data brokers, and, possibly, some advertising networks) on the one hand, and firms that otherwise use data as part of their operations (everyone else).

A. Valuing data for data brokers and ad networks

Data as a commodity is worth very little – so little it is potentially onerous to generally require firms to maintain an accounting of it. Moreover, it is very difficult to actually put a price on data.⁴¹ When data brokers and other intermediaries in the digital economy do try to value data, the prices are almost uniformly low. For example, according to the Financial Times,

[g]eneral information about a person, such as their age, gender and location is worth a mere \$0.0005 per person, or \$0.50 per 1,000 people. A person who is shopping for a car, a financial product or a vacation is more valuable to companies eager to pitch those goods. Auto buyers, for instance, are worth about \$0.0021 a pop, or \$2.11 per 1,000 people... Knowing that a woman is expecting a baby and is in her second trimester of pregnancy, for instance, sends the price tag for that information about her to \$0.11... For \$0.26 per person, buyers can access lists of people with specific health conditions or taking certain prescriptions... [T]he sum total for most individuals often is less than a dollar.⁴²

The reason for these low valuations is because data is a specific asset, meaning it has “a significantly higher value within a particular transacting relationship than outside the relationship.”⁴³ Data only appears valuable because the firms that *use* the data are so valuable. In reality, it is the combination of high-skilled labor, large capital expenditures, and cutting-edge technologies (e.g., machine learning) that makes those companies so valuable.⁴⁴ Yes, data is an important component of these production functions. But, in reality, it makes little sense to claim that the data possessed by firms have little, if any, independent value.

Thus, where data itself is a commodity the price is close to zero.

⁴¹ Will Rinehart, *How Do You Value Data? A Reply To Jaron Lanier's Op-Ed In The NYT*, THE TECHNOLOGY LIBERATION FRONT, Sep. 23, 2019, <https://techliberation.com/2019/09/23/how-do-you-value-data-a-reply-to-jaron-laniers-op-ed-in-the-nyt/>.

⁴² Emily Steel, *Financial worth of data comes in at under a penny a piece*, FINANCIAL TIMES, June 12, 2013, <https://www.ft.com/content/3cd056c6-d343-11e2-b3ff-00144feab7de>

⁴³ Benjamin Klein, *Asset Specificity and Holdups* in THE ELGAR COMPANION TO TRANSACTION COST ECONOMICS (Peter G. Klein & Michael E. Sykuta, eds.) available at http://masonlec.org/site/files/2012/05/WrightBaye_klein-b-asset-specificity-and-holdups.pdf

⁴⁴ See, e.g., Dan Gallagher, *Data Really Is the New Oil*, WALL STREET JOURNAL, Mar. 9, 2019, <https://www.wsj.com/articles/data-really-is-the-new-oil-11552136401>

B. Valuing data for general firms

Although the proposed allowance for “[a]ny other practical and reliable method of calculation used in good-faith”⁴⁵ allows the AG’s Office a degree of latitude when confronted with the inevitably vast differences across use cases for data that will surely arise, even such an extremely liberal *potential* allowance will do little to mitigate the chilling effect that this regulation will impose on general firms.

When data, as noted above, either eludes valuation or is practically worthless in isolation, firms face a stark choice: collect only the minimum data required to operate in an effort to comply with the CCPA, or take a legal risk by collecting more than is strictly necessary where that data *might* be useful to later innovations developed by the firm.

If the problem is framed strictly from the perspective of maximizing a social value of privacy, this may not sound like a problem at all. But, of course, the real world is not so simple. “Privacy” is only *one* value in a network of competing values that are implicated by technology and the use of data.

To begin with, there are clear benefits to information sharing that must be taken into account. Since the dawn of the Internet, free digital services have created significant consumer surplus and this trend continues today: Recent research using both survey and experimental methodologies has consistently found substantial benefits for consumers from sharing information in exchange for free (or subsidized) digital products.

Allcott et al., for example, studied the price that Facebook users were willing to accept in order to abstain from using the service for four weeks.⁴⁶ In the study, the median willingness-to-accept (“WTA”) from participants was \$100.⁴⁷ The WTA estimate means that “[a]ggregated across an estimated 172 million US Facebook users, the mean valuation implies that four weeks of Facebook generates \$31 billion in consumer surplus in the US alone.”⁴⁸

Corrigan et al. reported similar results of “a series of three non-hypothetical auction experiments where winners are paid to deactivate their Facebook accounts for up to one year.”⁴⁹ In their conclusion, the researchers said, “Though the populations sampled and the auction design differ across the experiments, we consistently find the average Facebook user would require more than \$1,000 to deactivate their account for one year.”⁵⁰

Brynjolfsson et al. reviewed the benefits of “several empirical examples [of technology that implicates privacy concerns] including Facebook and smartphone cameras” and then “estimate[d] their valuations

⁴⁵ Proposed California Consumer Privacy Act Regulations § 999.337(b)(8).

⁴⁶ Hunt Allcott, Luca Braghieri, Sarah Eichmeyer, and Matthew Gentzkow, *The Welfare Effects of Social Media*, NBER Working Paper No. 25514 (2019).

⁴⁷ *Id.* at 5. Note, this was not just cheap talk—the study followed through and paid a randomly-selected portion of the users to deactivate their accounts for four weeks. *Id.*

⁴⁸ *Id.*

⁴⁹ Jay R. Corrigan et al., *How much is social media worth? Estimating the Value of Facebook by Paying Users to Stop Using It*, PLOS ONE (2018).

⁵⁰ *Id.*

through incentive-compatible choice experiments.”⁵¹ The study found considerable benefits that are currently excluded from national accounts: “For example, including the welfare gains from Facebook would have added between 0.05 and 0.11 percentage points to GDP-B growth per year in the US.”⁵²

In a literature review of the economics of privacy, Acquisti et al. concluded that:

Extracting economic value from data and protecting privacy do not need to be antithetical goals. The economic literature we have examined clearly suggests that the extent to which personal information should be protected or shared to maximize individual or societal welfare is not a one-size-fits-all problem: the optimal balancing of privacy and disclosure is very much context-dependent, and it changes from scenario to scenario.⁵³

Moreover, what we think of as privacy is actually an umbrella covering many related concepts, each with their own separate complicating factors.⁵⁴ As some economists have aptly pointed out:

If our perusal of the theoretical economic literature on privacy has revealed one robust lesson, it is that the economic consequences of less privacy and more information sharing for the parties involved (the data subject and the actual or potential data holder) can in some cases be welfare enhancing, while, in others, welfare diminishing.⁵⁵

With this in mind, digital privacy regulations can have important unintended consequences that could significantly harm consumer welfare in the long run. These include misunderstanding consumer preferences, requiring excessive data protection, mandating business models, imposing compliance costs that potentially exceed benefits of those regulations, crowding out superior privacy offerings stemming from the private sector, and protecting some companies’ market power.

Further, it’s important to underscore that, even in the face of all the potential innovation that can come from new uses of data, it is typically out of the reach of firms to be able to actually place a value on any piece of data. The studies noted above refers to a WTA as expressed by *consumers*. The asymmetry of the relationship between consumers and providers means that providers generally will not have access to any particular user’s WTA.

But more to the point, as noted above, it is the combination of the business’s processes with data that enable it to generate value, and that revenue generation will not be even across all users’ data. Some data will end up being more valuable in a given business process, and other data valuable in a different context. Thus, the actual value of the data won’t actually emerge until the data is employed.

⁵¹ Erik Brynjolfsson et al., *GDP-B: Accounting for the Value of New and Free Goods in the Digital Economy*, NBER Working Paper No. 25695 (2019).

⁵² *Id.*

⁵³ Alessandro Acquisti, Curtis R. Taylor, and Liad Wagman, *The Economics of Privacy*, 52(2) J. ECON. LIT. 48 (2016) (emphasis added).

⁵⁴ Alessandro Acquisti, Curtis R. Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442, 443 (2016).

⁵⁵ *Id.* at 462.

The implications for the present regulation are complicated. In some cases, firms will be able to produce outputs with data inputs that are very valuable, and in other cases the data will never end up being valuable at all. Thus, in order to anticipate *potential* value that *might* be realized, a firm faces two choices. First, it can report average revenue per user, and smooth the differences in revenue generation over its entire user base where it expects large outliers (extremely high value and extremely low value users) to be rare. Second, if it anticipates that a small group of users will end up generating a large amount of its revenue, it has a reasonable incentive to report a very large “valuation” of every piece of data, despite the fact that *most* of its users’ data will be nearly worthless.

The choice is essentially arbitrary from the firm’s perspective and doesn’t actually provide real information about a particular user’s data. Nonetheless, regulators should be careful not to read too much into the numbers, and likely, should treat an extremely wide range of potential valuations as having been reasonably made in “good faith.”

III. Recommendations

We offer the following suggestions as points where implementation of the CCPA could be improved.

A. Modify the definition of “personal information”

Under the CCPA protected “personal information”

means information that identifies, relates to, describes, **is capable of being associated with, or could reasonably be linked, directly or indirectly,** with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household[.]⁵⁶

As Professor Goldman has observed, under this definition “what doesn’t qualify as personal information in the CCPA?”⁵⁷ Outside of one narrow exception for information provided publicly by the government, essentially *all* information remotely related to an individual qualifies as “personal information” because every such piece of information is “capable of being associated with, or could reasonably be linked” with that individual.

Moreover, since the definition of “personal information” includes both information about an individual as well as information about his or her household, conflicts in how to apply the law are inevitable. Different individuals in a single household do not always (or usually) have strictly aligned interests.⁵⁸ Therefore, the AG’s Office needs to carefully consider how to avoid allowing one member of a household to access or modify the private information of other members of the household.

⁵⁶ California Civil Code § 1798.140(o) (1) (emphasis added).

⁵⁷ Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, Santa Clara Univ. Legal Studies Research Paper 3 (2019) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013

⁵⁸ *Id.* (“These people’s interests may diverge, such as with separating spouses, multiple generations under the same roof, and roommates”).

In order to avoid overinclusive enforcement, as well as data breaches and privacy invasions by members of households against each other, the definition of “personal information” needs to be interpreted more narrowly.

If the definition is to have a reasonable meaning, it cannot be interpreted to mean *any* information at all that could remotely be used to identify an individual. For example, entries of user activity in various web site logs, and other observational data about the behavior of website users should not be interpreted as “personal information.” At the same time, the AG’s Office should clarify that different members of households do *not* have access or modification rights to the information of *other* members of the household. Further, and related to the broader point about over-inclusivity, a household member’s web activity that generates observations about, for instance, the behavior of certain IP Addresses should not be treated as the “personal information” of all members of the household.

B. Liberally interpret the “value” of data

As noted above, placing a realistic estimate of value on any particular piece of data is a fraught exercise. In proposed regulation 999.337 (“Calculating the Value of Consumer Data”) the AG’s Office should include an acknowledgement that any estimates provided will be understandably imprecise. Further, given the highly imprecise nature of performing such calculations, the AG’s Office should emphasize that it will interpret “good faith” compliance liberally.

C. Clarify the definition of “business”

The difference between a business that merely “receives” consumer information and one that “buys,” “sells,” or “shares” consumer information is large. Further, even the ostensibly large threshold of “50,000 or more consumers” is trivial to reach under the existing interpretations. Any service that passively recorded information on at least 137 residents of California per day becomes subject to the law. There should be a meaningful distinction between firms that buy and sell information as a commodity, and those that merely collect information about user behavior as an aspect of their business.

Therefore, the AG’s Office should clarify that § 1798.140(c)(1)(B) does not mean that any firm that “receives for the business’s commercial purposes” an individual’s personal information includes firms that merely “receive” information on consumers as a normal part of operations. For example, a service that logs a user’s behavior through a site “receives” location, IP Address, and other information about that user, but should not be included in such a broad definition.

D. Ensure there exists reliable user verification methods

In order to work properly, the CCPA depends on the AG's Office requiring that firms use systems that can validate "verifiable consumer requests."⁵⁹ A "verifiable consumer request" is defined as

a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify... to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer... if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General... that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.⁶⁰

This is a critical piece of the law. If the verification procedures are not carefully designed, the CCPA transforms from a law designed to protect privacy into a law that facilitates identity theft, hacking, and fraud. And, particularly given the very broad definition of "personal information" noted above, businesses will have a difficult time verifying many consumer requests without requiring consumers to disclose *more* information about themselves to the firms.

For example, if the broad definition of a business that merely "receives" information remains as-is, and the broad definition of "personal information" similarly remains, websites with little or no direct relationship with a given individual have no internal means for validating a particular consumer's request. Faced with this dilemma, businesses either need to require that consumer to provide extensive enough documentation to allow validation – thus paradoxically requiring consumers to expose *even more* sensitive information to discover if any information on them exists at all – or the businesses need to err on the side of disclosure. But erring on the side of disclosure introduces the risk of leaking information to malicious third parties.

This is a very real concern. In the wake of GDPR, faced with ambiguity around validating users requesting data, some firms have been shown to improperly provide information on their users. In one highly publicized incident, a security researcher set about to find out how much of his fiancée's information he could fraudulently obtain using GDPR requests.⁶¹ Although large tech companies tended to field his requests as expected, mid-sized businesses with less resources to handle GDPR requests performed poorly.⁶² Ultimately, out of 83 firms that the researcher attempted to exploit:

⁵⁹ See California Civil Code § 1798.100(c).

⁶⁰ California Civil Code § 1798.140(y).

⁶¹ Leo Kelion, *Black Hat: GDPR Privacy Law Exploited to Reveal Personal Data*, BBC NEWS, Aug. 8, 2019, <https://www.bbc.com/news/technology-49252501>

⁶² *Id.*

- 24% supplied personal information without verifying the requester's identity
- 16% requested an easily forged type of ID that he did not provide
- 39% asked for a "strong" type of ID
- 5% said they had no data to share, even though the fiancée had an account controlled by them
- 3% misinterpreted the request and said they had deleted all her data
- 13% ignored the request altogether⁶³

California would be well advised to avoid exposing the information of its citizens to similar data security risks. The AG's Office should therefore delay implementation of the CCPA until such time as it can verify that there are adequate, widely available means for firms of all sizes to validate consumer information requests. At the same time, it would be advisable to seek amendments from the California legislature that create better guidelines around how such verification procedures should work given the troubling evidence emerging from the EU around its similar privacy program.

E. Delay implementation until jurisdictional boundaries are clear

Finally, despite the DC Circuit trimming the FCC's 2018 Restoring Internet Freedom Order,⁶⁴ the fact remains that the FCC still retains a conflict-preemption authority to specifically preempt state laws that are incompatible with its regulations.⁶⁵ To wit,

Conflict preemption applies to “state law that under the circumstances of the particular case stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress—whether that ‘obstacle’ goes by the name of conflicting; contrary to; repugnance; difference; irreconcilability; inconsistency; violation; curtailment; interference, or the like.”

The DC Circuit only limited the FCC's ability to *generally* preempt potentially conflicting state laws, requiring that each preemption be challenged in a fact-intensive inquiry.⁶⁶

Similarly, it is also possible that the broad extent of the CCPA's rules, and their impositions on firms outside of California's borders could lead to Dormant Commerce Clause challenges.⁶⁷ Activities that “inherently require a uniform system of regulation” or that “impair the free flow of materials

⁶³ *Id.*

⁶⁴ *Mozilla Corp. v. Fed. Commc'ns Comm'n*, *supra*, note 13.

⁶⁵ *Id.* at 81.

⁶⁶ *Id.*

⁶⁷ *See, e.g., Graham Owens, supra*, note 17.

and products across state borders” violate the Dormant Commerce Clause.⁶⁸ As the FCC noted in its Restoring Internet Freedom Order, Internet-based communications is such a type of activity.⁶⁹

Therefore, the AG’s Office should consider using its authority to “[e]stablish[] any exceptions necessary to comply with state or federal law”⁷⁰ to temporarily delay implementation of the CCPA until latent federal preemption issues can be resolved. In particular, the AG’s Office should determine that (1) the contemplated implementation of the CCPA does not violate the Dormant Commerce Clause and (2) the AG’s Office has the opportunity to consult with the FCC and ensure that the implementation of the CCPA is not subject to conflict-preemption in light of the authority of the FCC’s over Internet communications.

On a related note, the AG’s Office should also consider harmonizing implementation of the law with other broadly applicable privacy laws, even where not legally compelled to do so. With the current structure of the CCPA, for example, businesses are not able to recycle their GDPR compliance programs.⁷¹ If there must be a state level data protection law, then it would be desirable to harmonize it with existing regulations elsewhere (in a manner that is less – not more – restrictive) in order to promote efficiency and clarity for consumers.

IV. Conclusion

Attached is a comment our center submitted to the National Telecommunications and Information Administration on the subject of developing a regulatory approach to privacy. The comment goes into the law and economics of privacy regulation in depth, but some high-level thoughts are appropriate to note here as the AG’s Office considers its implementation of the CCPA.

Although the US does not have a single, omnibus privacy regulation, this does not mean that the US does not have “privacy law.” In the US, there already exist generally applicable laws at both the federal and California level⁷² that provide a wide scope of protection for individuals, including consumer protection laws that apply to companies’ data use and security practices, as well as those that have been developed in common law (property, contract, and tort) and criminal codes.

⁶⁸ Ark. Elect. Co-op. Corp. v. Arkansas Pub. Serv. Comm’n, 461 U.S. 375, 384 (1984).

⁶⁹ RIF Order, *supra*, note 19, ¶ 200.

⁷⁰ California Civil Code § 1798.185(3)

⁷¹ Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, Internet Association of Privacy Professionals, Jul. 2, 2018, <https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/>

⁷² See, e.g., California Civil Code § 1798 et seq. (California data breach law).

In addition, there are specific regulations pertaining to certain kinds of information, such as medical records,⁷³ personal information collected online from children,⁷⁴ credit reporting,⁷⁵ as well as the use of data in a manner that might lead to certain kinds of illegal discrimination.⁷⁶

Getting regulation right is always difficult, but it is all the more so when confronting evolving technology, inconsistent and varied consumer demand, and intertwined economic effects — all conditions that confront online privacy regulation. Given this complexity, and the limits of our knowledge regarding consumer preferences and business conduct in this area, the proper method of regulating privacy is, for now at least, the course that the Federal Trade Commission has historically taken: case-by-case examination of actual privacy harms, without *ex ante* regulations, coupled with narrow legislation targeted at problematic uses of personal information.

Many (if not most) services on the Internet are offered on the basis that user data can, within certain limits, be used by a firm to enhance its services and support its business model, thereby generating benefits to users. To varying degrees (and with varying degrees of granularity), services offer consumers the opportunity to opt-out of this consent to the use of their data, although in some cases the only way effectively to opt-out is to refrain from using a service at all.

U.S. privacy regulators have generally evidenced admirable restraint and assessed the relevant tradeoffs, recognizing that the authorized collection and use of consumer information by data companies confers enormous benefits, even as it entails some risks. Indeed, the overwhelming conclusion of decades of intense scrutiny is that the application of *ex ante* privacy principles across industries is a fraught exercise as each firm faces a different set of consumer expectations about its provision of innovative services, including privacy protections.

This does not mean that privacy regulation should never be debated, nor that a more prescriptive regime should never be considered. But any such efforts must begin with the collective wisdom of the agencies, scholars, and policy makers that have been operating in this space for decades, and with a deep understanding of the business realities and consumer welfare effects involved.

Thank you again for the opportunity to comment on these timely and important topics.

⁷³ See, e.g., The Health Information Portability and Accountability Act (“HIPAA”), 45 CFR Parts 160 and 164.

⁷⁴ See, e.g., Children’s Online Privacy Protection Act (“COPPA”), 16 CFR Part 312.

⁷⁵ See, e.g., Gramm-Leach-Bliley Act, 15 USC § 6801.

⁷⁶ See, e.g., Civil Rights Act of 1968, Title VIII (“Fair Housing Act”), 42 U.S.C. 3601, et seq.

Appendix



Comments on Developing the Administration's Approach to Consumer Privacy

International Center for Law & Economics

Authored By:

Geoffrey A. Manne, President & Founder

Kristian Stout, Associate Director

Dirk Auer, Senior Fellow

I. Introduction

We thank NTIA for the opportunity to comment on this timely and highly relevant policy discussion. Digital privacy and data security are important ongoing concerns for lawmakers, particularly in light of recent, high-profile data breaches and allegations of data misuse. Understandably, in the wake of such incidents advocates regularly call for tighter restrictions on data collection and use. But, as we detail below, privacy is a highly complex topic comprising a wide variety of differing, and often conflicting, consumer preferences. While undoubtedly in need of ongoing assessment in the face of new challenges, the US federal government's sectoral, tailored model of privacy regulation remains the soundest method of regulating privacy.

We have seen other jurisdictions recently experimenting with different methods of arranging and deploying privacy regulations: most notably, the EU's General Data Protection Regulation ("GDPR")¹ and the California Consumer Privacy Act ("CCPA").² In the course of this Request for Comment ("RFC") (and for some time before it), advocates have sought to influence the US to follow the lead of these jurisdictions and enact legislation mandating tight controls on private companies' use of consumer data akin to those of the GDPR.³ We believe it would be a mistake to take this approach.

Although the US does not have a single, omnibus, privacy regulation (like the GDPR), this does not mean, that the US does not have "privacy law." In the US, there already exist generally applicable laws at both the federal and state level that provide a wide scope of protection for individuals, including consumer protection laws that apply to companies' data use and security practices,⁴ as well as those that have been developed in common law (property, contract, and tort) and criminal codes.⁵ In addition, there are specific regulations pertaining to certain kinds of information, such as medical records, personal information collected online from children, credit reporting, as well as the use of data in a manner that might lead to certain kinds of illegal discrimination.⁶

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679>.

² The California Consumer Privacy Act of 2018, 2018 Cal ALS 55, 2017 Cal AB 375, 2018 Cal Stats. ch. 55, available at <https://www.isipp.com/resources/full-text-of-the-california-consumer-privacy-act-of-2018-ccpa/>.

³ See, e.g., Letter of Johnny Ryan, Chief Policy & Industry Relations Officer, Brave, to David J. Redl (Nov. 6, 2018), available at <https://brave.com/ntia-federal-privacy-law/Submission-to-US-National-Telecommunications-and-Information-Administration-Dept.-Commerce.pdf>; Justin Joffe, *Apple's Tim Cook Proposes U.S. Version of GDPR at Data Protection Conference*, PR NEWS, Oct. 10, 2018, available at <https://www.prnewsonline.com/apple-tim-cook-communicators-us-gdpr>.

⁴ See, e.g., FTC Act, 15 U.S.C. § 45(a) et seq.

⁵ PRIVACY-COMMON LAW, <http://law.joink.org/pages/9409/Privacy-Common-Law.html> (last visited Nov. 8, 2018).

⁶ As the Association of National Advertisers notes: "[T]he Health Information Portability and Accountability Act ("HIPAA") regulates certain health data; the Fair Credit Reporting Act ("FCRA") regulates the use of consumer data for eligibility purposes; the Children's Online Privacy Protection Act ("COPPA") addresses personal information collected online from children; and the Gramm-Leach-Bliley Act ("GLBA") focuses on consumers' financial privacy; the Equal Employment Opportunity Commission ("EEOC") enforces a variety of anti-discrimination laws in the workplace including the Pregnancy Discrimination Act ("PDA") and American with Disabilities Act ("ADA"); the Fair Housing Act ("FHA") protects against discrimination in housing; and the Equal

In principle the EU's aggressive new data regulations are based on distinct cultural realities: The EU and its member states have long recognized a fundamental right to privacy and data protection that does not have an analog in the US.⁷ Yet, even before adoption of the GDPR in 2016, the EU and its member states operated for the last several decades under the same Charter of Fundamental Rights, but with less restrictive privacy regulations. As the Internet grew in popularity, the EU passed the ePrivacy Directive and the E-Commerce Directive, which established a more or less comprehensive framework of privacy principles that members states would have to implement.

But the GDPR is not a mere extension from the previous practice of the EU; rather, it is a new venture in comprehensive, centralized privacy regulation. It is certainly possible that such a new regulatory venture is wise and warranted, particularly as a manifestation of the EU Charter on Fundamental Rights. But it is also true that—as evidenced by EU practice before the GDPR and under each member state's national data protection authority—the protection of even a fundamental right to privacy does not necessarily dictate any particular form of regulation. Indeed, the Court of Justice of the EU (CJEU) has declared that “[t]he right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society.”⁸ Further, the CJEU held that

Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.⁹

It thus would seem that, even in the EU, competing and pragmatic considerations must be weighed against any particular data protection regime.

This is only more true in the US. In contrast to the EU, a fundamental right to privacy does not exist in the US.¹⁰ The US has, in some circumstances, regarded certain types of privacy as

Credit Opportunity Act (“ECOA”) protects against discrimination in mortgage and other forms of lending.” Comments of the Association of National Advertisers on the Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201, at 6, available at <https://docplayer.net/93116976-before-the-federal-trade-commission-washington-dc-documents-of-the-association-of-national-advertisers-on-the.html>.

⁷ Article 8.1 of the European Charter of Fundamental Rights, entered into force in 2009, provides that “[e]veryone has the right to the protection of personal data concerning him or her.” Charter of Fundamental Rights of the European Union art. 8.1, 2000 O.J. C 364/10, available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Article 8.1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed into force in 1950, provides that “[e]veryone has the right to respect for his private and family life, his home and his correspondence.” European Court of Human Rights, <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c>. (last visited Nov. 9, 2018).

⁸ Volker und Markus Schecke GbR & Harmut Eifert v. Land Hessen, Joined Cases C-92-93/09, [2009] E.C.R. I-11063, ¶ 48, available at <http://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=en>.

⁹ *Id.* ¶ 50.

¹⁰ More accurately, American and European traditions with respect to the role and understanding of privacy in society are significantly divergent: Whereas “Continental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*[. . .]. . . America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state.” James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004), available at <https://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty>.

fundamental, typically as against intrusion by the government,¹¹ but it has generally developed a culture of toleration for what may in other countries constitute privacy invasions by private persons or firms.¹²

This distinction, among others, counsels strongly against the emulation of the EU’s privacy regulatory regime in the US.

Before engaging in a deeply interventionist regulatory experiment, there should be empirically justifiable reasons for doing so; in the language of economics, there should be demonstrable market failures in the provision of “privacy” (however we define that term), before centralized regulation co-opts the voluntary choices of consumers and firms in the economy.

But neither the GDPR nor the CCPA provide any detailed analysis demonstrating that firms are failing to deliver the optimal level of privacy protections based on the various tradeoffs that consumers actually face. It surely might be the case that some consumers, abstractly speaking, would prefer one-hundred percent perfect privacy and security. It is also a certainty that, faced with tradeoffs—including the price of services, the number of features, the pace of innovation, ease of use and convenience—consumers are willing to settle for some lesser degree of privacy and security.

The responsibility of legislators who wish to write legislation that optimizes that set of tradeoffs is two-fold. First, there must be a demonstration that actual failures to provide optimal privacy and security exist, *relative to consumers’ revealed preferences*. Second, there must also be a demonstration that new legislation will not introduce new costs that dwarf the value they are designed to create.

As we detail below, the available evidence suggests that, at least at this time, there is no demonstrable failure in the market’s provision of privacy protection or the existing legal regime’s ability to regulate it. Moreover, the experimental and theoretical literature also demonstrates that many of the proposed regulatory interventions are at best useless, and at worst destructive.

Getting regulation right is always difficult, but it is all the more so when confronting evolving technology, inconsistent and heterogeneous consumer demand, and intertwined economic effects that operate along multiple dimensions – all conditions that confront online privacy regulation:

[S]ecuring a solution that increases social welfare[] isn’t straightforward as a practical matter. From the consumer’s side, the solution needs to account for the benefits that consumers receive from content and services and the benefits of targeting ads, as well as the costs they incur from giving up data they would prefer to keep private. Then from the ad platform’s side, the solution needs to account for the investments the platform is making in providing content and the risk that consumers will attempt to free ride on

¹¹ See, e.g., *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Lawrence v. Texas*, 539 U.S. 558 (2003) (fundamental right to privacy in substantive due process); *Carpenter v. U.S.*, 138 S. Ct. 2206 (U.S. 2018) (cell tower tracking violates expectation of privacy under Fourth Amendment).

¹² Compare Restatement (Second) of Torts § 652B Comment c (1977) (“Nor is there liability for... taking [someone’s] photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye.) with Elisabeth Logeais & Jean-Baptiste Schroeder, *The French Right of Image: An Ambiguous Concept Protecting the Human Persona*, 18 LOY. L.A. ENT. L.J. 511, 514-15 (1998) (Describing foundational French cases where permission from a subject must first be obtained before her image could be taken or displayed).

those investments without providing any compensation—in the form of attention or data—in return. Finally, the solution must account for the costs incurred by both consumers and the ad platform including the costs of acquiring information necessary for making efficient decisions.¹³

Given the complications confronting privacy regulation, and the limits of our knowledge regarding consumer preferences and business conduct in this area, the proper method of regulating privacy is, for now at least, the course that the Federal Trade Commission (FTC) has historically taken, and which has, generally, yielded a stable, evenly administered regime: case-by-case examination of actual privacy harms and a minimalist approach to ex ante, proscriptive or prescriptive regulations, coupled with narrow legislation targeted at unambiguously problematic uses of personal information. Following this approach will allow authorities to balance flexibility and protection.

This approach to privacy protection matches the United States' historic preference for light-touch regulation when dealing with highly dynamic markets. The Internet in the United States grew up around an ethos of “permissionless innovation”¹⁴ in which firms were free to experiment with business models and service offerings, and consumers were essentially free to interact with those services they found valuable relative to the costs, both in terms of money and, relevant here, in terms of personal data.

This environment has been and continues to be essentially based on “opt-out.” Many (if not most) services on the Internet are offered on the basis that user data can, within certain limits, be used by a firm to enhance its services and support its business model, thereby generating benefits to users. To varying degrees (and with varying degrees of granularity), services offer consumers the opportunity to opt-out of this consent to the use of their data, although in some cases the only way effectively to opt-out is to refrain from using a service at all. Over time online services have generally increased the extent of user control over the use of user data, and the type of controls have evolved as both technology and consumer preferences have changed. This trend appears to mirror general consumer preferences with respect to privacy,¹⁵ and this evolution of business practice has concomitantly shaped user expectations regarding privacy online.¹⁶

U.S. privacy regulators have generally evidenced admirable restraint and assessed the relevant trade-offs, recognizing that the authorized collection and use of consumer information by data companies confers enormous benefits, even as it entails some risks. Indeed, the overwhelming conclusion of decades of intense scrutiny is that the application of ex ante privacy principles across industries is a

¹³ David S. Evans, *Mobile Advertising: Economics, Evolution and Policy* at 45 (June 1, 2016), available at <http://ssrn.com/abstract=2786123>.

¹⁴ See A. THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (Mercatus Center George Mason University. 2016).

¹⁵ See Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns*, 102 AM. ECON. REV. PAPERS & PROCEEDINGS 349 (2012) (Reporting the results of empirical research demonstrating that: “(1) Refusals to reveal information have risen over time, and (2) Older people are much less likely to reveal information than are younger people. Our data further suggest that though younger respondents have become somewhat more private over time, the gap between younger and older people is widening”).

¹⁶ See Adam Thierer, Public Interest Comment on Federal Trade Commission Report, Protecting Consumer Privacy in an Era of Rapid Change (Arlington, VA: Mercatus Center at George Mason University 2011, 25). (Thierer lists a number of areas where competition between firms has spurred privacy protection).

fraught exercise as each industry — indeed each firm within an industry — faces a different set of consumer expectations about its provision of innovative services and offering of privacy protections.

This background reality does not mean that privacy practices and their regulation should never be debated, nor that a more prescriptive regime should never be considered. But any such efforts must begin with the collective wisdom of the agencies, scholars, and policy makers that have been operating in this space for decades, and with a deep understanding of the business realities and consumer welfare effects involved.

II. Privacy Regulation, Market Failures, and Regulatory Restraint

In evaluating the contours of possible privacy legislation it is crucial first to ask why—and even whether—such legislation is needed. And before imposing regulatory burdens it is crucial to question the underlying merits of politicized claims and political movements that may purport to represent overwhelming consumer interests but that may, in fact, do nothing of the sort.

Thus a vital question in the privacy protection space is whether and why markets operating without specific privacy regulation lead to a sub-optimal provision of privacy protection. Without starting with this inquiry, it is unclear what problems legislation is needed to address; and without knowing its purpose, any legislation is likely to be ineffective, at best, and may in fact make things worse, by increasing costs for consumers and businesses alike, mandating harmful prescriptions for alleged privacy harms, or exacerbating the risks of harm—or all of the above.

Particularly in the US, where privacy is treated both legally and socially as more of a consumer preference (albeit perhaps a particularly important one) than a fundamental right,¹⁷ it is difficult to determine whether our current regime produces the “right” amount of privacy protection. It is not enough that advocates and particularly privacy-sensitive consumers think there should be more, nor is it enough that there have been some well-publicized violations of privacy. Indeed, the fact that revealed preferences in the market tend toward relatively *less* privacy protection is evidence that advocates (and some legislators) may be seeking to create privacy protection for which there is simply no demand, beyond their own idiosyncratic preferences. Absent a pervasive defect that suggests a broad disconnect between revealed and *actual* preferences,¹⁸ and given the costs, we should be extremely cautious about adopting more invasive regulation.

With this in mind, it is important to look at the purported market failures that have been put forward to justify the adoption of privacy regulations. Doing so offers a hint as to whether privacy regulation is filling critical gaps in the market or whether, instead, certain elements of privacy regulation are white elephants that may cost more to society than the limited benefits they bring.

¹⁷ Except, of course, where it comes to *government* access to private information, e.g., under the Fourth Amendment. See *supra* notes 10-12 and accompanying text.

¹⁸ And some of these have indeed been suggested, as we discuss in this section, *infra*.

A. The Conditions that Potentially Justify Privacy Regulation and the Likelihood of their Occurrence

1. Information asymmetry

One potential privacy failure stems from the fact that consumers may be insufficiently informed about firms' use of their personal information and about the potential risks that this entails. If this were the case, we would likely expect to see either or both of the following scenarios unfolding: **(Error! Reference source not found.)** services offering relatively higher levels of privacy protection exit the market because of adverse selection; or (b) consumers offering "too much" private information because they underprice the costs associated with sharing data. Both of these outcomes are unlikely to occur in practice.

The notion that information asymmetries can lead to a "market for lemons" in which only lower quality goods or services are offered for sale was famously formalized by George Akerlof in his Nobel-winning article.¹⁹ Akerlof argued that when products vary in quality but buyers are unable to ascertain the quality of a good before they make a purchase, potential sellers of higher quality goods will be unable to capture their investment in quality. As a result, such sellers will exit the market (or never enter) and the average quality of goods on the market will be lower than would be the case if buyers could ascertain quality in advance.

This phenomenon is generally referred to as "adverse selection." The underlying intuition is that, because buyers cannot ascertain a good's actual quality, their reserve price is based on its expected quality. This discourages firms from selling high quality goods because they cannot obtain superior revenue from them. In turn, this further decreases the average quality of the goods that are sold. This has a knock-on effect on the price that consumers are willing to pay and the pool of goods that is sold.

Some authors have recently voiced concerns that something similar might be occurring in the case of personal data.²⁰ They argue that consumers are unable to ascertain the quality of a firms' privacy policy *ex ante*. As a result, firms may have insufficient incentives to introduce consumer-friendly policies.²¹

There are problems with this story, however. First and foremost, firms' privacy policies are generally hidden in plain sight. For users that really care about privacy, all the information they require is readily available. And it is hardly any more of a secret when firms change their privacy policies: experts pay attention to these changes, summarize them, and pass them through to consumers in

¹⁹ See George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970).

²⁰ See, e.g., Tony Vila, Rachel Greenstadt & David Molnar, *Why We Can't Be Bothered to Read Privacy Policies*, ECONOMICS OF INFORMATION SECURITY 143 (2004).

²¹ *Id.*

more easily digestible formats. A recent example of this phenomenon occurred when the GDPR go-live date was approaching, and articles about privacy policy updates abounded.²²

But even less obvious privacy policy changes have previously garnered popular attention. Electronic Frontier Foundation, a digital rights advocacy organization, has tracked changes to Facebook's privacy policy for years, to take one example.²³ And in response to this scrutiny, Facebook has made changes over the years to accommodate user concerns.²⁴ Of course, Facebook has also made other mistakes in its handling of user data—Cambridge Analytica, to take one recent example—but even in that case, the failures that occurred were discovered after the company had *already* changed the way it altered data in order to alleviate user concerns.

To the extent that consumers actually care about the privacy of their information, and short of fraud or deception (both of which are addressed by existing tort, consumer protection, and criminal laws), they are able to find out what policies apply to their information and to take steps to mitigate if needed. In some cases this means simply refusing to interact with a service that offers an insufficient take-it-or-leave-it privacy policy. Indeed if concern for privacy is sufficiently strong, even a mere *lack* of information about a services' policies can induce users to exit the market, thus pushing against the market for lemons.

In other cases, however, the reality of consumer knowledge means simply employing the widely available self-help tools that address most users' concerns. Most users "pay" for online services by having their data collected and then seeing targeted ads or having that information sold for other uses. Those who wish to avoid such data collection or use must generally pay for the products directly, but often they have options to do just that. Among other things, those consumers can generally pay by purchasing services that don't collect or use data in objectionable ways (for example, self-hosted or other paid email services instead of Gmail) or by using services that may have lower quality or other, different characteristics, but that don't collect data (for example, search engines that don't collect data but may not be as effective as those that do). Similarly, there are a number of third-party mechanisms (like ad-block applications, VPNs, or incognito browsing) that can minimize the exposure of data at some cost to underlying product functionality.

The entities that supply these third-party services, of course, have strong incentives to ensure that users are aware of the privacy practices of the primary services they frequent, and thus they, too, assist in overcoming any information asymmetries that may persist. Meanwhile, the FTC and other consumer protection regulators undertake to educate consumers regarding privacy and data security

²² See, e.g., Arielle Pardes, *What is GDPR and Why Should You Care?*, WIRED, May 24, 2018, available at <http://www.wired.com/story/how-gdpraffects-you/>.

²³ See, e.g., Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELECTRONIC FRONTIER FOUNDATION, Apr. 28, 2010, available at <https://www.eff.org/deeplinks/2009/12/facebook-s-new-privacy-changes-good-bad-and-ugly>; <https://www.eff.org/deeplinks/2010/04/facebook-timeline>; Kurt Opsahl & Rainey Reitman, *The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads*, ELECTRONIC FRONTIER FOUNDATION, Apr. 22, 2013, available at <https://www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads>.

²⁴ Juliette Garside, *Facebook bows to pressure on privacy setting for new users*, THE GUARDIAN, May 22, 2014, available at <https://www.theguardian.com/technology/2014/may/22/facebook-privacy-settings-changes-users>.

risks and mechanisms to address them,²⁵ and have undertaken numerous enforcement actions against firms that they believe have misled or defrauded consumers with respect to the use of personal information.

The unlikelihood of a market for lemons in privacy is compounded by the fact that most online consumers are best viewed as repeat purchasers. Users of social networks, such as Facebook, Instagram, and LinkedIn, generally provide new information on a regular basis. As soon as a platform uses consumers' data in a way that harms them, those same consumers are more likely to defect if they believe the firm is likely to continue its substandard protection of data. The #DeleteFacebook campaign in the wake of the Cambridge Analytica data breach demonstrates this consumer response.²⁶

Furthermore, it is not always the case that offering more privacy protective services is more expensive for firms, and thus they may in some cases have an incentive to offer them even without pressure from consumers. For example, retaining consumer data for long periods of time increases the costs of storage; collecting, storing, and processing more and different types of data is expensive, and in many cases it is not readily monetizable.

Consider the manufacturer that exercises market power by skimping on quality in order to pad profits. Why do profits increase when, for example, a cookie maker uses less sugar or inferior cocoa powder, or an automobile manufacturer uses low quality paint or electronics? *Ceteris paribus*, profits rise because inferior inputs tend to mean lower costs. In this manner, a reduction in quality with the price held constant is analogous to an increase in price.

Contrast this situation with an online publisher that decides to collect and mine additional consumer data. Distinct from the reduction in quality scenarios above, the online publisher does not profit automatically by reducing consumer privacy. Taking additional consumer data is not the same as skimping on quality, because collecting, storing, and analyzing data is an *additional cost*.²⁷

While it is certainly true that this dynamic may have limited effect where data may simply be sold or where its very use is part of the services offered (e.g., many social networks), it remains the case that the adverse selection effect is dampened to the extent that “lower quality” does not equate with “lower price.”

It must be noted, however, that lack of full information *can* lead to a potential “moral hazard” problem. In this case, the information that consumers may lack (or care sufficiently about) concerns other people or broader public goods. Under these conditions, users may share too much information or

²⁵ See, e.g., Federal Trade Commission Consumer Information, <https://www.consumer.ftc.gov/topics/privacy-identity-online:security> (last visited Nov. 8, 2018).

²⁶ Tiffany Hsu, *For Many Facebook Users, a 'Last Straw' That Led Them to Quit*, N.Y. TIMES, Mar. 21, 2018, available at <https://www.nytimes.com/2018/03/21/technology/users-avoid-facebook.html>.

²⁷ James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1135 (2013).

willingly take on too much risk of information exposure—the so-called “moral hazard”—either because they don’t know of the effect beyond themselves, or because they don’t internalize these costs.

In the modern data economy it is often the case that data about one person can reveal information about other people; the Cambridge Analytica kerfuffle demonstrated this. A study by MIT students showed that men’s sexual orientation can be predicted by an analysis of social network sites such as Facebook, even if they do not share information about their sexuality. In this case, the inference was possible because data analytics reveal that homosexual men have proportionally more gay friends than straight men, which allows one to predict sexual orientation based solely on the sexuality of their friends (information that the friends may have revealed, even if a particular user chose not to).²⁸

Given certain data that may correlate with certain personal characteristics, it is possible that information about a person can be gleaned, at least to some extent, from information shared by others. It may also be the case, for similar reasons, that national security or the protection of other interests (say, trade secrets) could also be compromised to some extent by the sharing of data, and thus that these interests may also not be sufficiently taken account of in individuals’ data sharing decisions.

This externality may be positive or negative, and, of course, the sign and magnitude of the effect can depend upon users’ idiosyncratic privacy preferences with respect to each aspect of information. Which effect predominates overall or in any particular instance is unclear. While advocates of strong privacy protections assume that negative externalities predominate, there really is no reason to think this is correct, and there is no evidence that we know of to suggest it is. Indeed, while there may be externalities from the collection and use of personal information, there are also externalities from *limits* on them to the extent they contribute to innovation. As Jones and Williams have shown, the social benefits of R&D are significantly larger than the internalized, private benefits.²⁹

And, at the same time, individuals’ preferences to *withhold* information or otherwise prevent it being shared may not account for the benefits such sharing would confer, even in cases where most of us would agree that the information at issue seems precisely the sort that should be protected. To take one example from a recent FTC workshop on the issue,³⁰ consumers may (understandably) strongly prefer to keep hidden from their social network connections ads that could appear indicating that the user purchased a home HIV test kit, if such data is used by the network to target ads to the users’ connections. It may be that the revelation that the user bought an HIV test imposes a high cost on the user. But it may also be that the revelation would alert the user’s sexual partners to their risk of infection and cause them to take their own precautions. Under these circumstances, the net benefit from the sharing of the information may be quite positive, even though the user may not take account of those external benefits.

²⁸ See Justin P. Johnson, *Targeted advertising and advertising avoidance*, 44 RAND J. ECON. 128 (2013).

²⁹ Charles I. Jones & John C. Williams, *Measuring the Social Return to R&D*, 113 Q. J. ECON. 1119 (1998) (estimating that the social return to R&D investment far exceeds the private return, meaning existing incentives for innovation are already lower than optimal).

³⁰ FTC Workshop on Informational Injury, Transcript at 84-86 (Dec. 12, 2017), *available at* https://www.ftc.gov/system/files/documents/public_events/1226463/informational_injury_workshop_transcript_with_ind_ex_12-2017.pdf.

2. The ignorance of consumers

Relatedly, the ignorance of users regarding the purported importance of threats to their personal information has been suggested as another justification for relatively more-heavy-handed, mandated privacy protections. At the core of this concern is that it is not just that consumers are unable to properly ascertain whether a firm will protect their personal information, but, more fundamentally, they might not even be aware that privacy protection and data security are relevant or important issues.³¹ Under this framing, mandating privacy disclosures and other default behaviors (like opt-in) by firms not only serves to inform consumers about each firm's specific privacy policy, but also to raise awareness about privacy issues in general and provide presumptive protections against over-sharing that runs counter to consumers' actual best interests.

However, the idea that most (or even many) consumers are entirely ignorant of privacy issues seems at odds with current developments in the area of privacy protection. The fact that the Cambridge Analytica scandal occupied the front pages of newspapers for weeks, slowed user growth on the Facebook platform, and wiped billions off Facebook's market capitalization is a testament to the importance that consumers attach to privacy issues.³²

Of course, a small minority of consumers may indeed be ignorant of privacy issues. Thankfully, they will almost certainly be protected by the operation of the relatively more privacy-conscious consumers existing in the same market. An analogy with the monopoly pricing of traditional goods is useful here. Just because one consumer has an exceedingly high valuation for a good does not mean that firms, even monopolists, will be able to extract that agent's entire consumer surplus. Monopolies almost systematically leave some buyers with consumer surplus. To attract marginal consumers, a monopolist must forgo profits on its inframarginal users (i.e. charge them a price that is lower than their reserve).³³ This remains true so long as the monopolist cannot perfectly price discriminate at reasonable cost. A similar dynamic applies to so-called "contracts of adhesion," which, although typically unread and un-negotiated by the majority of consumers, nevertheless are found to offer largely efficient combinations of terms and prices because they must offer competitive terms to the particularly sensitive (marginal) consumers who *do* read them.³⁴

The same logic applies to privacy protection. Although a small subset of users may be totally ignorant of privacy issues, firms cannot cash in on this ignorance because they are unable to identify these ill-informed users and write-up a separate privacy policy for them. This applies *a fortiori* when there is competition between online firms to attract them. Just as consumers do not need to shop around to get competitive prices in markets for physical goods, each individual does not have to be aware of a firm's privacy policy to benefit from competitive terms.³⁵ In other words, a committed minority of

³¹ See Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016).

³² See Rupert Neat, *Over \$119bn wiped off Facebook's market cap after growth shock*, THE GUARDIAN, July 26, 2018, available at <https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollar-after-growth-shock>.

³³ See H.R. VARIAN, MICROECONOMIC ANALYSIS 236 (W.W. Norton, 1992).

³⁴ See, e.g., Douglas G. Baird, *The Boilerplate Puzzle*, 104 MICH. L. REV. 933, 936 (2006) (noting that "[t]he sophisticated buyer provides protection for those that are entirely ignorant").

³⁵ See Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, U. CHI. LEGAL F. 207, 214-15 (1996) ("[I]t is foolish to complain about contract terms. These all are mediated by price. 'Better' terms (as buyers see things) support higher prices,

privacy-conscious individuals enable relatively less informed agents to enjoy a competitive level of privacy protection.

The virtuous influence that highly-informed consumers exert on their peers is likely to be even more pronounced when markets present network effects, as is often the case with online platforms. Network effects occur when a consumer's utility for a good is, at least in part, a function of the expected number (and quality) of other agents using the same product.³⁶ Although it is often mentioned that network effects are self-reinforcing (adding users to a network will attract even more users), the inverse is also true. One group of users leaving a network may cause the whole platform to enter a "death spiral."³⁷ For this reason, online platforms are likely to be particularly wary of losing users for privacy-related reasons. More generally, the self-reinforcing nature of network effects also explains why user adoption is such a crucial metric for firms operating in the digital economy.³⁸

Finally, even if it transpires that consumers are globally ignorant of privacy issues, top-down regulation is still unlikely to be the solution. Two scenarios are possible. A first possibility is that users do not attach any value to privacy matters, even when they are perfectly informed. If this is the case, then there is no scope for privacy regulations to improve consumer welfare; consumers are simply indifferent to the use that is made of their personal information.

A second possibility is that users would attach some value to privacy matters if only they were properly informed—in other words, there is some latent demand for privacy protection. But, unless there are widespread monopoly market failures, firms have an incentive to ferret out this preference, seize upon this latent demand, and, because of the pressures of competition, provide the welfare-maximizing level of privacy protection. This second scenario seems to be supported by empirical evidence.³⁹

The upshot is that users being uninformed does not amount to a privacy market failure, so long as there is actual or potential competition for their patronage.

It is also important to recognize that apparent indifference to a variety of potential privacy harms may not, in fact, be the result of ignorance, but rather an informed preference. When consumers do decide to join or remain on a platform, it may be safe to assume—especially now that several high-profile data breaches have occurred—that their decisions to do so account for the expected losses that they may suffer with regards to their personal information.⁴⁰ In other words, these consumers

and sellers have as much reason to offer the terms consumers prefer (that is, the terms that consumers find cost-justified) as to offer any other ingredient of their products. It is essential to enforce these terms if markets are to work.”)

³⁶ See, e.g., Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93, 96 (1994).

³⁷ See David S. Evans & Richard Schmalensee, *Debunking the Network Effects Bogeyman*, 40 REGULATION 36 (2017). See also, Joseph Farrell & Paul Klemperer, *Coordination and lock-in: Competition with switching costs and network effects*, 3 HANDBOOK OF INDUSTRIAL ORGANIZATION, 63 (2007).

³⁸ See Michael L. Katz & Carl Shapiro, *supra* note 36, at 96.

³⁹ See generally Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. (2011).

⁴⁰ It is demonstrably true inasmuch as consumers continue to use Facebook, Google et al now that they know more about the potential for data breaches and misuse. However, in surveys consumers contradict themselves: Kimberly Collins, *As consumers expectations rise, brands find new data to personalize experience*, CLICKZ, Sept. 17, 2018, available at

are, at the very least, revealing that they value the services of a platform more than the expected “price” they might pay through the unauthorized revelation of their information. Barring severe information asymmetries (which seems implausible following the aforementioned data breaches),⁴¹ it is likely reasonable to conclude that data security issues are priced into consumers’ dealings with online platforms.

3. *Data monopolies*

Several of the dynamics discussed above turn on the presence of product market competition to ameliorate the effects of perceived defects like information asymmetry. Thus, the possibility that, at least in certain markets, “data monopolies” tend to emerge presents another potential justification for imposing relatively more onerous privacy requirements. The premise is that markets that rely heavily on consumer data are inherently prone to monopolization. This is notably said to stem from so-called “data network effects,” and allegedly results in insufficient privacy protection for users.⁴² A closer inspection of numerous digital markets suggests that this concern is overstated, however.

For a start, it is wrong to assume that data-intensive products necessarily lead to winner take all situations, akin to those that may occur in the presence of network effects. As Hal Varian aptly demonstrates, unlike network effects, data does not produce value in and of itself.⁴³ Instead, data must be analyzed to create value. As a result, companies cannot merely outcompete their rivals by acquiring superior or larger datasets: they must also hire the best data engineers and “learn by doing.”⁴⁴ Because of this, there is no necessary data “positive feedback loop” and an industry’s heavy reliance on data does not necessarily lead to higher concentration. For instance, brick and mortar retailers make heavy use of their consumers data and yet there is no reason to believe that these markets are particularly prone to concentration.

And, even where there are network effects, there is little reason to believe that this would make data-reliant markets less competitive. Although some scholars have voiced fears that network effects may lead to highly concentrated markets, not all markets with network effects will eventually tip towards a single winning firm.⁴⁵ Moreover, in those cases where network effects do lead to lopsided market distributions, potential competition from smaller competitors or new entrants may constrain the behavior of incumbents. In this case, the presence of network effects might merely substitute competition “in the market” with competition “for the market.”⁴⁶ In other words, these effects do not

<https://www.clickz.com/as-consumer-expectations-rise-brands-find-new-data-to-personalize-experience/216842/>. Once again, revealed preferences do not match elicited preferences.

⁴¹ See, *supra*, at notes 19-30, and accompanying text.

⁴² See Maurice E Stucke, *Should We Be Concerned About Data-opolies?*, 2 GEO. L. TECH. REV. 275, 283 (2018).

⁴³ See Hal Varian, *Artificial intelligence, economics, and industrial organization*, in THE ECONOMICS OF ARTIFICIAL INTELLIGENCE: AN AGENDA 15 (2018).

⁴⁴ *Id.*

⁴⁵ This is especially true in the presence of heterogeneous consumer preferences and differentiated products. See Shapiro & Katz, *supra* note 36, at 106.

⁴⁶ See Sami Hyrynsalmi, Arho Suominen & Matti Mäntymäki, *The Influence of Developer Multi-homing on Competition Between Software Ecosystems*, 111 J. SYS. & SOFTWARE 119, 119-27 (2016).

necessarily prevent entry by more-efficient and/or innovative rivals,⁴⁷ nor do they preclude the creation of another market entirely through disruptive innovation.⁴⁸ And, as the basic premise of this RFC demonstrates, privacy is certainly one dimension along which these firms continue to compete. There exist privacy-oriented alternatives to browsers⁴⁹ and search engines,⁵⁰ for example, and even in the cellphone market—which is often characterized as a duopoly of iOS and Android⁵¹—Apple touts its more protective approach to security and privacy as a major feature of its iPhones.⁵²

The notion that network externalities may benefit user privacy is also backed by economic findings concerning two-sided markets. In a highly acclaimed paper, Mark Armstrong has shown that competition between multi-sided platforms may result in particularly intense competition to acquire single-homing users (who are present on only one of many competing platforms).⁵³ This is often, though not always, the case for users of social networks, search engines, game consoles and of online retail platforms. Because there will be intense competition to attract these exclusive consumers (often resulting in zero nominal prices), any latent demand for privacy protection is likely to be met by competing firms.

There is thus little reason to believe that the presence of network effects would necessarily lead to inferior privacy protections for users. On the contrary, as has already been mentioned, network effects are a double-edged sword that are likely to result in platforms catering closely to the needs of privacy-conscious users and thus benefiting all other users on the network.⁵⁴

Moreover, there is reason to believe that the competitive process itself is fully capable of protecting privacy interests. In their empirical study of consumer preferences and firm behavior with respect to consumer privacy protections, Tsai et al. found that

businesses may use technological means to showcase their privacy-friendly privacy policies and thereby gain a competitive advantage. In other words, businesses may direct their policies and their information systems to strategically manage their privacy strategies in ways that not only fulfill government best practices and self-regulatory recommendations, but also maximize profits.⁵⁵

The market is the best disciplining force for correcting firms that stray from consumer preferences. Firms are driven by the profit motive, which is to say that if the non-ad supported, privacy-oriented products that already exist—and that comport with the notion of, for example, an opt-in regulatory requirement—were actually offering a service that consumers desired at a price they were willing to

⁴⁷ See E. Glen Weyl & Alexander White, *Let the Best "One" Win: Policy Lessons from the New Economics of Platforms*, 10 COMPETITION POL'Y INT'L, 28 (2014).

⁴⁸ See, e.g., Thibault Schrepel, *L'innovation de Rupture: De Nouveaux Défis Pour le Droit de la Concurrence*, 42 REVUE LAMY CONCURRENCE 141, 143 (2015).

⁴⁹ See, e.g., *About Us*, BRAVE, <https://brave.com/about/> (last visited Nov. 9, 2018).

⁵⁰ See, e.g., *DUCKDUCKGO*, <https://duckduckgo.com/about>.

⁵¹ Greg Sterling, *US Market Becoming a Smartphone Duopoly*, MARKETING LAND, July 23, 2018.

⁵² See, e.g., David Nield, *All the Ways iOS 12 Will Make Your iPhone More Secure*, WIRED, July 8, 2018.

⁵³ See Mark Armstrong, *Competition in two-sided markets*, 37 RAND J. ECON. 678 (2006).

⁵⁴ See Evans & Schmalensee, *supra* note 37.

⁵⁵ Janice Y. Tsai, et al., *supra* n. 39 at 266.

bear, those services would thrive, and the less privacy-sensitive options would be forced to shift their practices. No barriers to entry, regulatory impediments or the like prevent such services from operating or succeeding, other than, it seems, lack of consumer demand (particularly in light of the research noted above suggesting that firms would be willing to profit from providing greater levels of privacy).

Firms in technology-intensive industries, moreover, frequently find it difficult to maintain dominance in a market, which puts further pressure on those firms to compete on price and quality. The classic example is Schumpeterian competition, in which firms leapfrog one another in a series of short-lived monopolies, each achieved through technological advance and maintained only so long as the then-monopolist can maintain its advantage. While this may bear the superficial hallmarks of monopoly, such dynamic competition in technology markets is actually perfectly consistent with strong competition and procompetitive outcomes.⁵⁶ Each successive “winning” firm must be committed to investing its profits in developing new and better technologies in order to try to preempt or co-opt the next technological wave and maintain its position.

Further, particularly in markets characterized by high degrees of technological change, potential competition can operate as effectively as—or even *more* effectively than—actual competition to generate competitive market conditions:

[I]n industries... where technological change is rapid, competition for the market may provide more benefits to consumers than competition in the market. Where competition for the market is important, the number of competitors in the market at any point does not usefully measure the extent to which competitive processes underlie market behaviour.⁵⁷

As applied here, if privacy-protections are important to consumers, firms in technology-heavy industries that are competing for the market have a sharp interest in meeting that consumer demand. The fact that at any given time only a single, or only a few, firms comprise an industry does not mean that the industry is not responsive to consumers’ preferences—for privacy as for all other aspects of the products and services they consume.

a. Exploitative and anticompetitive data usage

Some scholars have argued that firms may use personal data to charge “exploitative” prices to consumers.⁵⁸ The claim is that this allegedly undesirable practice is facilitated by access to personal

⁵⁶ See, e.g., Thomas M. Jorde and David J. Teece, *Antitrust Policy and Innovation: Taking Account of Performance Competition and Competitor Cooperation*, 147 J. INST’L & THEORETICAL ECON. 118 (1991). Note also that “competition for the market” can be as constraining as within-market competition. See Harold Demsetz, *Industry Structure, Market Rivalry and Public Policy*, 16 J. L. & ECON. 1 (1973).

⁵⁷ Neil Quigley, *Dynamic Competition in Telecommunications: Implications for Regulatory Policy* 17, C.D. HOWE INSTITUTE COMMENTARY, no. 194 Feb. 2004, available at https://www.cdhowe.org/pdf/commentary_194.pdf. See also A.E. Kahn, *Telecommunications: The Transition from Regulation to Antitrust*, 5 J. TELECOMM. & HIGH TECH. L. 159 (2006); Jason Pearcey & Scott J. Savage, *Actual and Potential Competition in International Telecommunications* 4 (Working Paper, Oct. 21, 2015), available at https://www.montana.edu/jpearcey/papers/ISR_Web.pdf (“Overall, these results suggest that incumbent firms reduce their price when potential competition increases....”); Harold Demsetz, *Id.*

⁵⁸ See Stucke, *supra* note 42, at 293 (2018). See also, Curtis R Taylor, *Consumer Privacy and the Market for Customer Information*, RAND J. ECON. 631 (2004).

information that may allow firms to more effectively price discriminate, anticipate consumer demand, and charge supra-competitive prices despite there being ostensible competition in the market. There are important objections to these assertions.

First and foremost, critics routinely miss the fact that, absent significant barriers to entry, no firm can expect to earn supra-competitive profits for an indefinite period of time. This includes profits derived from data-driven price discrimination. The reason for this is straightforward. One firm earning high profits will inevitably attract entry from competitors and/or encourage consumers to switch towards rival firms. This arbitrage ultimately leads to lower prices and to more privacy practices that comport with user expectations as a quality dimension of competition.

Second, even if a firm could price discriminate without the threat of arbitrage, high-value consumers would have huge incentives to withhold their personal information and/or send deceptive signals that they are low-value purchasers. When this is the case, the ability to acquire detailed consumer information may, counterintuitively, lead to lower prices and higher consumer welfare.⁵⁹

III. The Costs of Departing From Current US Privacy Regulations

All regulation comes at a cost. Even well-intentioned regulation designed to protect the privacy of individuals must be evaluated in terms of both the benefits it provides to individuals as well as the costs to those same individuals, the firms they contract with, and social welfare. Moreover, protecting “privacy” is not a straightforward task: What we think of as privacy is actually an umbrella covering many related concepts, each with their own separate complicating factors.⁶⁰ As some economists have aptly pointed out:

If our perusal of the theoretical economic literature on privacy has revealed one robust lesson, it is that the economic consequences of less privacy and more information sharing for the parties involved (the data subject and the actual or potential data holder) can in some cases be welfare enhancing, while, in others, welfare diminishing.⁶¹

With this in mind, digital privacy regulations, such as the GDPR and the CCPA, can have important intended and unintended consequences that could significantly harm consumer welfare in the long run. These include misunderstanding consumer preferences, requiring excessive data protection, mandating business models, imposing compliance costs that potentially exceed to benefits of those regulations, crowding out superior privacy offerings stemming from the private sector, and protecting some companies’ market power.

B. Opt-in Versus Opt-out

The most significant and problematic deviation from existing US practice exhibited by the GDPR and CCPA approaches is the switching of the default presumption concerning data use from “opt-out” to “opt-in” for a significantly expanded class of data.

⁵⁹ See Taylor, *supra* note 58, at 643 (2004).

⁶⁰ Acquisti, et al., *supra* note 31, at 443.

⁶¹ *Id.*, at 462.

The problem is that “[opt-in] provides no greater privacy protection than ‘opt-out’ but imposes significantly higher costs with dramatically different legal and economic implications.”⁶² In staunching the flow of data, opt-in regimes impose both direct and indirect costs on the economy and on consumers,⁶³ reducing the value of certain products and services not only to the individual who does not opt-in, but to the broader network as a whole. Not surprisingly, these effects fall disproportionately on the relatively poor and the less technology-literate.⁶⁴

Furthermore, empirical research shows that opt-in privacy rules reduce competition by deterring new entry. Thus, the seemingly marginal costs imposed on consumers by requiring opt-in can have a significant cumulative effect on competition: “[R]ather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive.... [I]n some cases where entry had been profitable without regulation, [some firms] will choose not to enter.”⁶⁵

For these reasons, when data usage is consistent with “the context of the transaction or the company’s relationship with the consumer,” regardless of the sensitivity of the data involved, the FTC does not generally require even choice, let alone affirmative consent, before a company collects or uses consumer data.⁶⁶ For those data uses that do fall outside the context of the transaction, the FTC requires “affirmative express consent” (opt-in consent) *only* for uses of particularly sensitive data.⁶⁷

An opt-in requirement effectively implies a determination that unauthorized data uses are presumptively harmful. But the mere fact that a consumer’s information may be used in ways that the user doesn’t expect or understand does not mean that such use is harmful to consumers individually or in the aggregate. Whether such uses are desirable, or on net are beneficial or harmful to consumers, is enormously context- and person-specific. But it does seem to be the case that presumptively deterring these transactions does *not* benefit consumers:

“Opt-in” is frequently portrayed as giving consumers greater privacy protection than “opt-out.” In fact, the opposite is true. **“Opt-in” provides no greater privacy protection than “opt-out” but imposes significantly higher costs with dramatically different legal and economic implications.**⁶⁸

⁶² Fred H. Cate & Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of “Opt-In”* at 1, available at <http://bit.ly/2kVZ9uz>. See also Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTED 155 (Apr. 2010), available at <http://bit.ly/2kKv2s>.

⁶³ *Id.* at 5 (“[T]he ‘opt-out’ system sets the default rule to ‘free information flow’ and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an ‘opt-in’ system presumes that consumers **do not want** the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.”) (emphasis in original).

⁶⁴ See, e.g., Lucas Bergkamp, *The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER LAW & SECURITY REPORT 31, 38 (2002); *Opt-in Dystopias*, *supra* note 62, at § 5.1.

⁶⁵ James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 48-49 (2015) (emphasis added).

⁶⁶ FTC Privacy Report at 48.

⁶⁷ *Id.* at 60.

⁶⁸ See Cate & Staten, *Protecting Privacy in the New Millennium*: *supra* note 62, at 1.

Similarly:

[T]he opt-out regime produces better welfare results than the anonymity regime, which in its turn is better than the opt-in regime. Therefore, from a social welfare point of view, it matters whether opt out or opt in is adopted as the privacy standard.⁶⁹

And, of course, an opt-in regime is indeed more expensive than an opt-out regime.⁷⁰ As Fred Cate and Michael Staten detail, the costs can fall widely on both consumers and providers, can be significant, and can deter valuable information exchange:

[C]onsider the experience of U.S. West, one of the few U.S. companies to test an “opt-in” system. In obtaining permission to utilize information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.), the company found that an “opt-in” system was significantly more expensive to administer, costing almost \$30 per customer contacted. To gain permission to use such information for marketing, U.S. West determined that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, many U.S. West customers received more calls than in an “opt-out” system, and one-third of their customers were denied opportunities to receive information about valuable new products and services.⁷¹

As this example suggests, the crucial problem with an opt-in regime is that it stanches the flow of data, imposing both direct and indirect costs on the economy and on consumers:

An “opt-out” system presumes that consumers **do want** the convenience, range of services, and lower costs that a free flow of personal information facilitates, and then allows people who are particularly concerned about privacy to block the use of their information. Put another way, the “opt-out” system sets the default rule to “free information flow” and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an “opt-in” system presumes that consumers **do not want** the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.

In other words, an “opt-in” system sets the default rule to “no information flow,” thereby denying to the economy the very lifeblood on which it depends. Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must rebuild the pipeline by contacting one customer at a time to gain their permission to use information.

Consequently, an “opt-in” system for giving consumers control over information usage **is always more expensive than an “opt-out” system.**⁷²

⁶⁹ Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis Of Privacy Policies*, available at <https://www.econstor.eu/bitstream/10419/25876/1/521168813.PDF>.

⁷⁰ See Cate & Staten, *supra* note 62; Lundblad & Masiello, *Opt-in Dystopias*, *supra* note 62.

⁷¹ See Cate & Staten, *supra* note at 62, at 5.

⁷² *Id.* (emphasis in original).

Finally, empirical research shows that opt-in privacy rules deter competition by deterring new entry. The seemingly marginal costs imposed on consumers by requiring opt-in can have a significant cumulative effect on competition:

[M]ost privacy regulation requires firms to obtain one-time individual consumer consent to use consumer data (rather than the consent requests increasing with the amount of data used). Therefore, privacy regulation imposes transaction costs whose effects... will fall disproportionately on smaller firms. Consequently, rather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive.

* * *

[In] competition between a generalist firm offering products that appeal to a variety of consumer needs and a specialist firm offering a product that serves fewer consumer needs,... privacy regulation can preclude profitable entry by the specialist firm. Under regulation, the extra costs required to obtain consent mean that in some cases where entry had been profitable without regulation, the specialist firm will choose not to enter. The generalist firm then captures the whole market. This implies that privacy regulation can increase the advantage enjoyed by a large generalist firm. This deprives consumers of the higher-quality niche product offered by a specialist firm, which represents a loss that must be balanced against any gain to consumers due to the increased privacy.⁷³

Mandating opt-in, on its own, can be damaging enough, but laws like the CCPA compound the injury by disallowing firms to shift their pricing models in response. Businesses are forbidden from refusing to deal with consumers who decline to opt-in, or of even from charging them higher prices in spite of their lower overall profitability to the firm.⁷⁴ Such price controls effectively benefit those who choose to opt out of the use of their data, at the expense of those who do not opt out, and will inevitably result in lower levels of investment in innovation, to the detriment of all consumers.

C. Mandating Transparency and Fairness

While it may be true that many consumers are ill-informed,⁷⁵ it is not clear that a government-imposed mandate on companies to process information “lawfully, fairly and in a transparent manner”⁷⁶ will do anything to make consumers better informed. First, if a company is not behaving lawfully, then it is unclear that a government regulation will do anything to stop such unlawful behavior. Second, fairness is a highly subjective term open to interpretation—and abuse. Third, and perhaps most important, government mandates for “transparent” information processing are often counter-productive.⁷⁷ Consider the example of mandatory disclosures of information on packaged food, which have resulted in an over-abundance of information, leading to a decline in the use of such labels by consumers—and leading to further attempts to provide more useful and useable

⁷³ Campbell, Goldfarb & Tucker, *supra* note 65, at 48-49.

⁷⁴ Cal AB 375 § 1798.125. (a) (1).

⁷⁵ But, see, *supra*, notes 31 -40 and accompanying text.

⁷⁶ GDPR at Article 5 (1).

⁷⁷ See generally, Geoffrey A. Manne, *The Hydraulic Theory of Disclosure Regulation and Other Costs of Disclosure*, 58 ALA. L. REV. 473 (2007).

information on the part of food companies and governments, many of them also unhelpful.⁷⁸ Likewise, consider the mandatory disclosure requirements for financial transactions, which have led to an explosion of form-filling but done little to improve consumer decision-making and may have undermined it, due to the great length of many such disclosures and resultant information processing fatigue.⁷⁹

Further complicating matters, consumers' preference for privacy, and similarly the benefits they derive from sharing information or from less protective uses of their information by firms, vary throughout the population.⁸⁰ The relationship between privacy and quality is purely subjective:

Saying that a publisher's decision to collect and analyze additional data reduces the quality of its service is akin to saying that a restaurant's decision to replace corn with green beans on its menu lowers the quality of its food. These statements will likely be true for some, but are false for others. There is no right answer.⁸¹

This makes it problematic to adopt policies aimed at mandating increased privacy protections because, for many people, these policies will harm them, even as the very same policies will benefit others. The upshot is that it is unclear what fairness entails for data processors, and thus what it means to comply with such a requirement. This introduces significant discretion on the part of enforcers into the system. Whether their sense of fairness better comports with overall social preferences is perhaps even less likely.

D. Compliance Opportunity Costs

The enactment of privacy regulations will often involve substantial costs for firms. Compliance with legal requirements that go beyond optimal protection measures and may entail inefficient direct costs, and the costs of government reporting, erroneous enforcement, and vexatious litigation can be substantial. In general, at least some of these costs will be passed on to consumers, either in the form of higher prices, lower quality, or less innovation, and these costs can offset or wipe out any possible gains from greater privacy protections.

In addition to these direct and indirect costs, privacy regulations may also entail substantial opportunity costs. These costs include the redirection of firms' engineers, lost business opportunities, and forgone investments.

⁷⁸ J. E. Todd & J. N. Variyam, *The Decline in Consumer Use of Food Labels, 1995-2006*, Economic Research Report Nr. 63 (2006), available at <http://www.ers.usda.gov>; J. N. Variyam & J. Cawley, *Nutrition Labels and Obesity*, NBER Working Paper No. W11956 (2006); B. Wansink & P. Chandon, *Can "Low-Fat" Nutrition Labels Lead to Obesity?*, *J. Marketing Res.*, 43: 605-17 (2006); B. Wansink, S. T. Sonka, & C. M. Hasler, *Front-label health claims: when less is more*, 29 *Food Policy* 656-67 (2004).

⁷⁹ Angela A. Hung et. al., *EFFECTIVE DISCLOSURE IN FINANCIAL DECISIONMAKING* (RAND Corp., 2015) available at https://www.rand.org/content/dam/rand/pubs/research_reports/RK1200/RK1270/RAND_RR1270.pdf

⁸⁰ See, e.g., Kai-Lung Hui & I.P.L. Png, *The Economics of Privacy*, in *HANDBOOKS IN INFORMATION SYSTEMS, VOL. 1, ECONOMICS AND INFORMATIONAL SYSTEMS* 489 (Andrew B. Whinston & Terrence Hendershott, eds., 2006) (noting that "the key policy issue is not whether individuals value privacy. It is obvious that people value privacy. What is not known is how much people value privacy and the extent to which it varies").

⁸¹ Cooper, *Privacy and Antitrust supra* note 27, at 1138.

It has been estimated that American S&P 500 companies and UK FTSE 350 companies spent a combined total of \$9 billion to comply with the GDPR in the year running up to its entry into force alone, for example.⁸² These figures do not include the significant costs incurred by smaller firms, firms that originate from other countries, and the expenses that businesses will have to incur in the future to stay in compliance with the GDPR.

But the costs do not stop there. The adoption of the GDPR has not magically conjured up an army of engineers to ensure compliance with its provisions. Instead, there is a vast opportunity cost involved, as many engineers have been forced to spend significant amounts of their time working on these issues. This is time that could otherwise be put to more productive uses, such as better managing supply chains, improving existing products and user experiences, and developing new and innovative goods. It is impossible to put a precise number on this cost, though its potential breadth is significant (the GDPR has no *de minimis* carve outs, which means that even tiny companies must ensure they comply with its provisions).⁸³

It is also important to account for the effects of privacy regulation on firms' ability to adopt efficient business practices or to engage in data-based innovation. Data (information) regulation (as opposed to other types of regulation) is particularly likely to affect institutional structure. As Luis Garicano notes:

Organizations exist, to a large extent, to solve coordination problems in the presence of specialization. As Hayek pointed out, each individual is able to acquire knowledge about a narrow range of problems. Coordinating this disparate knowledge, deciding who learns what, and matching the problems confronted with those who can solve them are some of the most prominent issues with which economic organization must deal.⁸⁴

Regulations that affect how firms can collect, store, use and disseminate information may thus have significant effect on firm governance and organization.

This dynamic could manifest itself as companies simply choosing to collect and use less data, but it could mean a lot of other things as well. It could affect corporate organization (e.g., deterring vertical integration or creating "data firewalls" between different divisions of a company), encourage limits on the geographic scope of data collection or operation, affect the mechanisms for determining executive compensation, or (further) encourage jurisdictional considerations to dictate incorporation and principal place of business decisions. While choosing second-best options is rational from the perspective of regulated parties, it is nevertheless costly to society, both in terms of the firm's efficient operation relative to its operation in a viable alternative regulatory regime and to consumer welfare generally.

⁸² Oliver Smith, *The GDPR Racket: Who's Making Money From This \$ 9 bn Business Shakedown*, FORBES, May 2, 2018, available at <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#33232d9834a7>

⁸³ See GDPR Art. 2.

⁸⁴ Luis Garicano, *Hierarchies and the Organization of Knowledge in Production*, 108 J. POL. ECON. 874, 874 (2000).

To take just one example, privacy regulations could arguably make it harder for companies to price discriminate, even in those instances where this would be welfare-enhancing. The most obvious example is that of insurance markets.⁸⁵ At the extreme, protecting users' privacy may prevent firms from obtaining information relevant to the setting of insurance premiums and compensation amounts. To the extent that this prevents insurers from better aligning premiums and risk, it impedes the role of premiums in accurately signaling risk and encouraging risk reduction. Moreover, to the extent that insurance companies would find it difficult or impossible to use subscribers' smartphone or GPS data and the like in assessing risk, it would increase these firms' administrative costs and may preclude them from offering lower premiums.

At the same time, mandating opt-in consent before firms may use data in novel ways will, at the margins, deter experimentation and innovation by all firms. It will impede the ability of firms to offer innovative product improvements, but also even to monetize their current products and services through the use of consumer data. The end result may be higher direct prices for consumers as well as fewer quality improvements over time.

E. Crowding Out

Another unintended consequence of mandating certain modes of privacy protection is that regulation may preempt private entities from offering differentiated or even superior protection on their own.

This pitfall is notably illustrated by Blockchain technology's rocky relationship with Europe's GDPR. Blockchain is the fruit of efforts by some of the most privacy-conscious individuals on the planet. At its core, blockchain technology usually implies partial or even total anonymity. While the most successful distributed ledgers, such as Bitcoin and Ethereum, are not fully anonymous (the ledger of completed transactions is public, though the contents of each transaction is private),⁸⁶ other projects such as Monero and Zcash offer total privacy to their users.⁸⁷ Details aside, the distributed ledger industry is, in no small part, a reaction to fears about privacy and centralization in mainstream web services.⁸⁸

Given this, one could be forgiven for thinking that blockchain technology would obviously comply with the requirements set out in the GDPR. But nothing could be further from the truth. In fact, the GDPR could potentially present a significant stumbling block to the wider adoption of

⁸⁵ Acquisti, et al., *supra* note 31, at 470.

⁸⁶ See Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, at 6 (2008), at <https://bitcoin.org/bitcoin.pdf> ("The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.")

⁸⁷ See Griffin Knight, *Monero vs. Zcash and the Race to Anonymity*, MEDIUM, Feb. 28, 2018, <https://medium.com/coinmonks/monero-vs-zcash-and-the-race-to-anonymity-4322b0a9bd90>.

⁸⁸ See, e.g., Vitalik Buterin, *Privacy on the Blockchain*, ETHEREUM BLOG, Jan. 15, 2016, <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/>.

distributed ledger technology.⁸⁹ Indeed, some of the GDPR's requirements, such as the right to erasure and amendment, are virtually incompatible with the immutable nature of the blockchain ledger.⁹⁰

The fact that blockchain might not comply with the GDPR is a clear case of what Nassim Taleb calls "Wittgenstein's ruler." He observes that

[u]nless you have confidence in the ruler's reliability, if you use a ruler to measure a table you may also be using the table to measure the ruler. The less you trust the ruler's reliability, the more information you are getting about the ruler and the less about the table.⁹¹

In the case at hand, the fact that blockchain technology does not comply with the strenuous requirements of the GDPR says more about the regulation's rigidity and its inability to adapt to new technology (even though it has only just entered into force) than it does about blockchain's lack of privacy protection.

Privacy regulation may also crowd out self-help products. These technologies and companies enable consumers to withhold data, send signals they are low-value purchasers, and exert more granular control over data. High profile examples of these technologies include ad blockers and VPNs. By potentially negating the need (or the perceived demand) for these products, regulation may effectively drive these firms out of business—firms whose specialized research and development may potentially yield relatively more optimal degrees of protection.

All of this has important downsides. In effect, regulation will shift the burden and decision-making regarding privacy protection from consumers, notably by using third-party products, onto online platforms operating under strict constraints. This may lead to both inadequate privacy protection and protection provided at a higher cost.

Unlike government intervention, which can misread potential demand for a given set of protections, self-help technologies act as revealed preferences. Their success or failure conveys valuable information about the type and quantity of privacy protection that is actually important to users. In turn, firms can monitor the success of these products and incorporate valuable privacy features into their own offerings. Arguably this is what has happened with browsers incorporating ad blockers, for example.

To make matters worse, by imposing command and control obligations on firms, regulation ignores the possibility that they might not be the least cost avoiders. In other words, it is plausibly more efficient for society to encourage users to withhold their personal information than to force firms to put in place costly measures designed to protect it. By legally preventing firms and consumers from reallocating the rights that exist between them, the strictest privacy regulations may ultimately harm consumers and firms alike.

⁸⁹ See Michèle Finck, *Blockchains and data protection in the european union*, 4 EUR. DATA PROT. L. REV. 17, 33 (2018).

⁹⁰ *Id.*

⁹¹ See N.N. TALEB, *FOOLED BY RANDOMNESS: THE HIDDEN ROLE OF CHANCE IN LIFE AND IN THE MARKETS* 224 (Random House Publishing Group 2008).

F. Entrenching Incumbent Firms

Finally, the adoption of privacy regulation may also have a significant effect on competition. Not only do these regulations potentially favor large incumbents over innovative startup companies, they may also induce firms to make costly choices regarding the business models that will prevail in affected sectors.

For a start, numerous economists have pointed out the privacy regulation tends to entrench established incumbents. For instance, Campbell, Goldfarb and Tucker show that “a potential risk in privacy regulation is the entrenchment of the existing incumbent firms and a consequent reduction in the incentives to invest in quality. These incentives are stronger when firms have little consumer-facing price flexibility, as is the case in online media.”⁹² Indeed, “privacy regulation can shield a large, general incumbent from potential competition because regulation raises the threshold quality and scope for profitable entry by a challenger.... This is more likely for relatively strong incumbents: the stronger the incumbent, the better the marginal entrant must be.”⁹³ This applies with even more force when privacy regulations rely on opt-in consent, because users are less likely to test the products of new entrants.⁹⁴

Another potential issue is that privacy regulations may lead firms to adopt differentiated business models (or advocate for regulations supporting them) not for their intrinsic value but for their ability to reduce their own costs relative to other firms, and to increase those of their rivals. Apple CEO, Tim Cook, appeared to evidence this dynamic in his reaction to the introduction of the GDPR. Cook publicly came out in favor of this type of regulation, calling for the United States to adopt similar provisions.⁹⁵ Unsurprisingly, he forgot to mention that Apple’s business model is far less reliant on personal data than those of its rivals, such as Google and Facebook, because it is not in the business of targeted advertising.⁹⁶ Apple thus stands to lose far less from the adoption of privacy regulations than its close rivals.

This last issue would not be much of an issue if all consumers unambiguously preferred Apple’s business proposition to that of its rivals, but this simply is not the case. Take smartphones, for instance. Whereas Apple offers the most high-end smartphones with more privacy protection (less exposure to targeted advertising), Google has differentiated itself by producing an OS that relies on targeted search engine advertising to generate profits (the Android OS).⁹⁷ This type of differentiation is potentially valuable for consumers. Privacy-conscious users can pay extra money to obtain the most secure device, while targeted advertising on the Android OS decreases the direct cost of devices for

⁹² See James Campbell, Avi Goldfarb & Catherine Tucker, *supra* note 65, at 68.

⁹³ *Id.*

⁹⁴ *Id.* at 49. See also, Jan Bouckaert & Hans Degryse, *Default Options and Social Welfare: Opt in Versus Opt Out*, 169 J. INSTITUTIONAL AND THEORETICAL ECON. JITE 468-489 (2013).

⁹⁵ See Russell Brandom, “Tim Cook wants a federal privacy law – but so do Facebook and Google”, THE VERGE, Oct. 24, 2018, available at <https://www.theverge.com/2018/10/24/18018686/tim-cook-apple-privacy-law-facebook-google-adpr>.

⁹⁶ See, e.g., Mehreen Khan, “Apple and Facebook call for EU-style privacy laws in US”, THE FINANCIAL TIMES, Oct. 24, 2018, available at <https://www.ft.com/content/0ca8466c-d1768-11e8-ab8c-0be0dcf18713>.

⁹⁷ See Dirk Auer, *Appropriability and the European Commission's Android Investigation*, 23 COLUM. J. EUR. L. 658 (2017).

more price-sensitive consumers. By arbitrarily preferencing a particular business model via privacy regulation, legislators may ultimately deprive consumers of valuable choices.

An *ex ante* requirement of a particular privacy model may, in fact, do much to discourage competition. Developing successful online platforms entails significant fixed costs; no magic switch exists to suddenly bring into existence a particular version of a software platform. Development of successful platforms entails hundreds or thousands of hours of engineering time—and mandating a platform that consumers don't seem to prefer means devoting that time to developing what the market has demonstrated to be an inferior product. Thus, the returns to such development will necessarily be less than the returns to development of the primary, ad-supported product possible under an opt-out default presumption, and, consequently, the ad-supported product will be forced to itself subsidize the legally-mandated paid version of the product.

For large, established platforms this cost can be (more or less) easily absorbed (depending, of course, on the underlying technology of the platform). But for startups such a regulatory obligation would amount to a significant entry barrier. In particular, the ability to gain critical mass for its service would be significantly reduced as its upfront fixed costs will explode, and its users will be spread across multiple services. The net result will be less entry (especially by smaller firms) and less-effective competition:

[A] specialist that fills a smaller niche and offers a smaller quality premium over the equivalent function of the generalist is more likely to earn lower revenue after entry in the case with regulation than in the case without.... Intuitively, absent regulation, entrants offer a targeted product after entry, and if the content of the firm's product offering has broad enough appeal, this generates enough revenue to allow them to profitably enter. With regulation... [s]maller entrants and entrants that offer a smaller quality premium in their niche are more likely to offer an untargeted product in equilibrium after entry. Since an untargeted product generates less revenue, this means that, all else equal, the marginally profitable entrant must be larger than before to overcome the fixed cost of entry....⁹⁸

These foregone benefits must be accounted for in assessing the full implications of more invasive privacy regimes. Imposing broad, general regulations regarding business models and privacy practices is a surefire way to curtail innovation and reduce overall competition. This inevitably will lead to a handful of large firms that are able to dominate a space as network effects will reinforce their success, and a lack of differentiation along privacy and advertising dimensions will discourage or outright forbid experimentation with novel business models.

IV. Conclusion

Thank you again for the opportunity to comment on these timely and important topics. Privacy is undoubtedly a critical topic for lawmakers to consider, and getting the mix of policies that best protect consumers, safeguard their expectations, and promote the growth of firms in the economy is challenging. Opportunities like these are invaluable for fully exploring this topic.

⁹⁸ Campbell, Goldfarb & Tucker, *supra* note 65.

Given the complications confronting privacy regulation, and the limits of our knowledge regarding consumer preferences and business conduct in this area, the proper method of regulating privacy is, for now at least, the course that the Federal Trade Commission (FTC) has historically taken, and which has, generally, yielded a stable, evenly administered regime: case-by-case examination of actual privacy harms and a minimalist approach to ex ante, proscriptive or prescriptive regulations, coupled with narrow legislation targeted at unambiguously problematic uses of personal information. For all its imperfections, following this approach will allow authorities to balance flexibility and protection, without stumbling into the unintended and harmful consequences that would surely arise from a more restrictive regulatory approach.

Message

From: Joanne Cooper [REDACTED]
Sent: 12/6/2019 7:12:47 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: nicklas.akers@dog.ca.gov
Subject: ID Exchange - CA DOJ CCPA Submission - 6 Dec 19
Attachments: ID Exchange - CA DOJ - Proposed CCPA Legislation Submission 6 Dec 19.pdf

Dear Privacy Regulations Co-ordinator,

To the California Office of the Attorney General, ID Exchange is pleased to submit the following correspondence in relation to the proposed California Consumer Privacy Act of 2018.

We also thank your Office for the opportunity to present at the San Francisco public hearing this week, it was greatly appreciated.

We look forward to continued communications in due course.

Kind regards,

[Joanne Cooper](#)

Founder - Managing Director

[ID Exchange Pty. Ltd.](#) A/NZ Representative of [digi.me Ltd.](#)

CBD Office | Stone & Chalk Incubator | Wynyard Green

L5 - 11 York Street - Sydney NSW 2000 - Australia

E: [REDACTED]

M: [REDACTED]

W: www.idexchange.me



This email communication could withhold confidential data information of ID Exchange Pty Ltd ACN 161437681. As such we request that if you are not the correct recipient of this communication that you must not therefore copy, keep, relay or rely, use, copy, save or forward this email distribution or communication. Unauthorised actions relating to this communication is prohibited and therefore if by chance you have received this in error please immediately discard this email and reply to the email sender to advise of the incorrect address delivery. Again please delete the received email communication and reply upon sending.



ID Exchange Pty Limited
 Stone & Chalk FinTech Incubator
 Wynyard Green
 11 York Street
 Sydney NSW 2000 Australia
 E: advisory@idexchange.me
 P: 1300 002 678
 ABN: 99 161 437 681
 www.idexchange.me

CONFIDENTIAL

California Department of Justice
Privacy Regulations Coordinator
 300 S. Spring St.
 Los Angeles, CA 90013
 CC: Office of Attorney General Xavier Becerra
 Email: privacyregulations@dog.ca.gov

6th December 2019

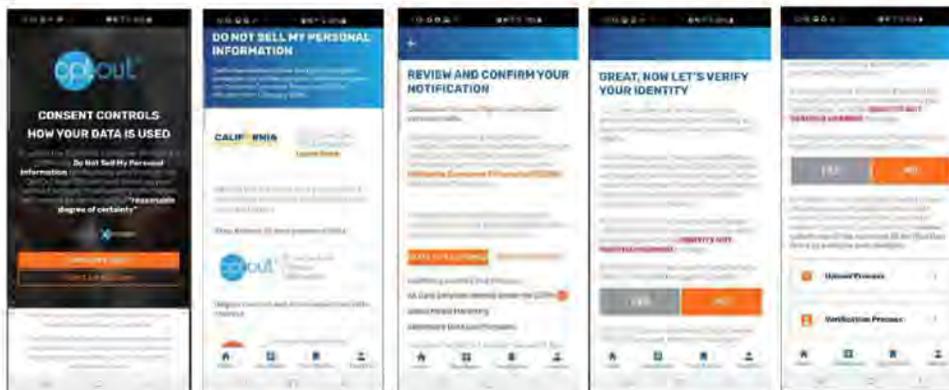
Dear CCPA Privacy Regulations,

We write in relation to the proposed legislation of the California Consumer Privacy Act of 2018 and in reference of the final public hearings held during December 2nd-5th 2019 to which I, Joanne Cooper of ID Exchange was pleased to present as speaker number three during the San Francisco December 4th hearing.

This submission supports the interest of ID Exchange to formerly meet with the State of California Depart of Justice in order to table and discuss ID Exchange’s portfolio of international trademarks / IP distribution holdings.

ID Exchange was established in 2012 to develop privacy enhancing technologies (PeTs) and digital rights management solutions to assist consumers to protect and mobilise their data for their benefit, this effort commenced well before the CA DOJ’s position on assisting Californians to protect their personal data assets from misuse.

Our IP and represented technology provides consumers with the means to control and manage their personal or sensitive data using methods such as unified instruments of consent management controls, which also utilise the form of OPT IN and OPT OUT® logos/buttons that activate various segments and specific compliance functionality. A representative image is provided below in our **Alpha** Opt Out® Mobile App for testing and pre-release refinement which is attuned to support the CCPA:



A verified Opt Out® request actioned via ID Exchange's Opt Out® App would instruct the Business (data holder) to de-identify your Personally Identifiable Information (PII) in a manner aligned to the CCPA regulation. This notification asks for the deletion of your name, address, email, gender, date of birth, contact number and any other PII data as stipulated under Privacy legislation. Often for this to be accepted by the data holder it must be compliant with data-collection "Do not sell my personal information or Opt Out" rules and the terms specific jurisdictional law. The App will also log consent receipts for Opt Out notices so that the Consumer is presented with a centralised dashboard in order for self-management and evidence of their Opt Out choices.

As previously informed, ID Exchange is the owner of U.S. Federal Trademark Registration No. 5,299,154 for the trademark OPT OUT and Design trademark depicted below for software related to Privacy, Digital Identity, SaaS and data rights management.



During January 2019 it came to ID Exchange's attention that the California Consumer Privacy Act of 2018 (CCPA) contains an early provision requiring the development of a uniform Opt Out logo. Section 1798.185(a)(4)(C) states that the Attorney General shall solicit comments on "[t]he 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."

Since informing the CA DOJ's that ID Exchange was concerned that Section 1798.185(a)(4)(C) may encourage the development of a logo or button that infringes upon its trademark rights in the Opt Out mark. This requirement then seemed to change to be re-stipulated as web site link – Do not sell my personal information.

However, we note that the recently released CCPA proposed regulations continues to reference in Article 2 - page:6 - Section 999.306. Notice of Right to Opt-Out of Sale of Personal Information – item E - Opt-Out Button or Logo

The commentary I presented at the San Francisco December 4th, 2019 hearing was to again seek more information about the continued reference of the CA DOJ's intention to activate an Opt Out logo/button and;

- When is the CA DOJ planning to release the design of this Opt Out button design for public comment? (*Clarification on this Opt Out logo/button was raised by other speakers at the SF public hearing.*)
- Is the CA DOJ interested in working with solution providers such as ID Exchange in the area of Privacy Enhancing technologies to provide consumer facing consent management services for citizens or the use of our Opt Out logo design/button technology?

As an innovative firm ID Exchange is greatly encouraged that the technology, intellectual property, and privacy by design technology that ID Exchange has been developing over several years which integrates world leading partnerships in the area of private data sharing, duty of care standards orchestrated to deliver seamless consumer centric services can accelerate the timely availability of tools aligned to meet the CCPA's legislation objectives to benefit all Californians and business.



We feel our IP holdings potentially strengthens the best form of execution so that this IP is utilised in an ethical manner with governance that does not constitute the vested interests of one BigTech firm over another through a distributed human centric ecosystem design which supports the intentions of such vital legislation for citizens.

Currently ID Exchange is engaged with the Australian Federal government and corresponding regulator as a stakeholder and working group participant due to the forming of the new Consumer Data Right Bill (CDR) which was recently passed by Parliament in an effort to deliver technologies aligned to emerging policy, privacy and data sharing legislation.

ID Exchange looks forward to commencing dialog and receiving guidance on how our investment, knowledge and IP assets may be of benefit to shape the State of California Government as an exemplar for wider US Federal Privacy legislation by exploring pathways to collaborate with Agencies or US firms to successfully utilise our IP in tune with such cornerstone Privacy legislation.

We strive to assure trusted personal information exchanges mobilise data as a raw material to compliantly flow within the Trillion-dollar personal data market.

Please advise at your earliest convenience your availability to discuss our questions at a suitable time.

Respectfully submitted,

Joanne Cooper
CEO, Founder
ID Exchange Pty Limited
M: [REDACTED]
E: [REDACTED]
W: www.idexchange.me



Message

From: Jeff Lokey [REDACTED]
Sent: 12/6/2019 12:15:05 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: dl Legal [Legal@infoblox.com]
Subject: Infoblox Inc. Comments re Notice of Proposed Rulemaking, Sections 999.300-341
Attachments: Infoblox NPRM Process Letter 12-05-19.pdf

Please see the attached letter submitted in connection with the Notice of Proposed Rulemaking, Sections 999.300-341.

Thank you in advance for your consideration. Please do not hesitate to contact us should you have any questions or wish to further discuss.

Respectfully submitted,

Jeff Lokey

Vice President, Legal Affairs

Direct - [REDACTED]

Mobile - [REDACTED]

www.infoblox.com



December 5, 2019

The Honorable Xavier Becerra
Attorney General of the State of California
600 West Broadway, Suite 1800
San Diego, CA 92101-3702

RE: Notice of Proposed Rulemaking, Sections 999.300-341

Dear Attorney General Becerra,

Infoblox Inc. is a Santa Clara, California-based technology company. Infoblox's proprietary hardware and software solutions protect the networks and sensitive data of government agencies, banks, airlines, healthcare networks, network service providers, academic institutions, and a majority of Forbes 1000 companies. This letter is respectfully submitted by Infoblox to provide comment and context regarding the Office of the Attorney General's Notice of Proposed Rulemaking ("NPRM") and proposed adoption of Sections 999.300-341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations ("CCR") concerning the California Consumer Privacy Act ("CCPA").

Specifically, we write to address the currently proposed definition of personal information under CCPA, which may be interpreted to include both static and dynamic IP addresses. Given that the CCPA is ultimately intended to protect California's citizens, our concern is that this current definition could have the unintended consequence of negatively impacting network security by limiting the ability of cybersecurity companies to use "Internet Protocol address(es)" to detect data security incidents or malicious activity. If this is allowed to occur, California's businesses and consumers will experience a decrease in their overall network security.

The concerning definition currently reads as follows:

(o) (1) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. . . .

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

See California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(o)(1) (2018).

To put this into context, Infoblox protects Domain Name System (“DNS”) (*e.g.*, when you type in a website address name your browser then directs you to the actual internet protocol address), infrastructure, automates cloud deployments, and increases the reliability of enterprise and service provider networks around the world via Dynamic Host Configuration Protocol (“DHCP”), and internet protocol address management (“IPAM”). Collectively, DNS, DHCP, and IPAM are known as “DDI.”

Modern attackers do not rely on a single, easily identifiable registered domain name to carry out their bidding, and instead create complex systems that automatically register hundreds or thousands of domain names and configure them to point to web servers that then distribute malicious content. Attackers change their domain names constantly to make it difficult to block them at a DNS level. Infoblox’s DDI solution identifies and counters these malicious attacks.

Since DNS and IPAM involve using “IP addresses” and “Internet or other electronic network activity” to enhance network security, cybersecurity companies including Infoblox are urging California to take into account the cybersecurity industry when it engages in this NPRM process for CCPA. The downside of not exempting business to business companies and cybersecurity providers from these regulations means that it will be far more difficult for these companies to operate in a manner that best protects the businesses and, by extension, the consumers of the State of California.

It is instructive to observe the increased regulatory complexity and uncertainty facing cybersecurity companies and domain name verification companies, such as Internet Corporation for Assigned Names and Numbers (“ICANN”), as a result of the broad-based definitions of personal data currently in place under GDPR. To compound matters, the European Court of Justice took an expansive view of personal data in relation to IP addresses in its ruling in Breyer, increasing administrative and financial burdens on the cybersecurity industry. We believe that the Breyer court did not have the opportunity to adequately consider and account for cybersecurity companies whose business it is to police and protect IP addresses to protect consumers and company networks. Ironically, there exists the very real threat the consumers will actually be rendered less safe. The goal of this letter is to ensure that California does not make the same oversight, and instead recognizes these important distinctions and carves out the exemptions necessary for cybersecurity companies to provide California consumers and businesses important network protections.

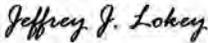
In light of the currently proposed definition of personal information in the NPRM process for CCPA, which includes an unqualified reference to “Internet Protocol address,” and the potentially detrimental consequences for critical network security created by such ambiguity, we respectfully request that the Attorney General take the following steps:

- (a) Clarify whether “Internet Protocol [“IP”] address” in § (o)(1) refers to static or dynamic IP addresses (or both)¹;
- (b) Consider how California should interpret “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household” in relation to IP addresses and “Internet or other electronic network activity information”² in light of the cybersecurity industry; and
- (c) Employ a balancing test for consumers’ interests whereby certain data fields like “Internet Protocol address” and “Internet or other electronic network activity information” only become personal information” if consumer’s privacy rights outweigh the benefit that consumers and/or society gain from the activity.

We are hopeful that California will adopt a considered approach as it works to define personal information in the context of IP addresses and electronic network activity under the CCPA. We are available at your convenience should you find it helpful to receive additional context or background on this letter or to answer any questions that you might have about our experience of navigating data privacy in the cybersecurity industry. We are available at your convenience and can be contacted via email at legal@infoblox.com or by telephone at (408) 986-4000.

Thank you in advance for your time and consideration.

Respectfully submitted,

DocuSigned by:

38CA2A73BFDA4CC...

Jeffrey J. Lokey
Vice President, Legal Affairs
Infoblox Inc.

¹ There are 2 different kinds of IP addresses available in the marketplace—static and dynamic addresses. “[I]nternet service providers allocate to the computers of internet users either a ‘static’ IP address or a ‘dynamic’ IP address, that is to say an IP address which changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider.” Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 2016 E.C.R. 779, available at <http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945> [hereinafter *Breyer*] at line 16. Indeed, dynamic IP addresses are “provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made, and not ‘static’ IP addresses, which are invariable and allow continuous identification of the device connected to the network.” *Id.* at line 36.

² California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(o)(1) (2018), available at https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.140.

Message

From: Scott Stewart [REDACTED]
Sent: 12/6/2019 1:30:27 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Innovative Lending Platform Association Comments on Proposed CCPA Regulations
Attachments: ILPA Comments on CCPA Proposed Regulations.pdf

Please see attached.



Innovative Lending Platform Association

December 5, 2019
Attorney General Xavier Becerra
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Dear Attorney General Becerra,

I am writing on behalf of the Innovative Lending Platform Association ("ILPA"), a leading trade organization representing a diverse group of online lending and servicing companies that provide financial products and services to small businesses, to share our concerns and requests for clarification of the proposed regulations for the California Consumer Privacy Act of 2018 ("CCPA").

Our members exclusively serve small businesses and are committed to expanding access to capital for small businesses across the country, particularly in areas underserved by traditional financial institutions. Between 2015 and 2017, five major online lenders, including several of our member companies, funded more than \$10 billion in loans to U.S. small businesses. In California, our member companies have provided over \$3 billion in capital to more than 35,000 small businesses.

Access to credit is critical for small businesses to grow. According to the annual 2019 small business credit survey conducted by 12 U.S. Federal Reserve, over half (53%) of small business credit applicants experienced a financing shortfall during the prior year. ILPA members fill this critical gap by leveraging technology, data and analytics to reduce transaction costs and power lending to small businesses.

We strongly believe in protecting our customers' data and treating the personal information of our customers carefully. We are highly supportive of the principles behind CCPA but have concerns about certain provisions of the proposed regulations that may have unintended impacts on our ability to provide much-needed capital to California small businesses.

Our concerns and recommendations are set forth below:

Providing Notice to Consumers

- **Notice at Collection of Personal Information**
 - As this is a legal notice, we request clarity on how we can accurately explain the required disclosures to the consumer without using at least some legal language.
 - Also, some categories of personal information, like cookies, are collected as soon as the consumer lands on the business's website, making it impossible to have this notice visible before any personal information is collected.

- **Privacy Policy**
 - We request additional guidance on how to accurately explain legal rights and obligations without using at least some legal language.
 - Our members are tech companies and it will be very difficult to avoid using technical jargon to describe their processing. While larger companies are able to do this, our members do not have access to the same resources that larger companies do to interpret, distill and present in plain language to consumers the technical aspect of the processing.

- We request clarification of the requirement for a “conspicuous link.” Does it need to be in large font? Is having it at the bottom of the page (today’s standard) sufficient to meet the conspicuous requirement?

Business Practices for Handling Consumer Requests

- **Methods for Submitting Requests to Know and Requests to Delete**
 - We believe that section (C)(2) goes beyond the scope of CCPA. The proposed regulations state that a consumer may request a covered entity delete any personal information collected or maintained by the business. We believe CCPA provides this right only to the extent that the information was collected directly from the consumer.
 - The proposed regulations list mail as an acceptable method for submitting requests to know and delete, but overlook a critical issue of postal mail when responding to requests to know and delete. Mail can be easily intercepted or lost. We request a reexamination of this requirement as it would be impossible to submit personal information to a consumer in the mail while also observing reasonable security measures.
 - We request clarity on the proposed regulation that would prevent, at any time, a business from disclosing certain specific pieces of information (e.g. social security numbers). Is it possible to disclose some portion of the information (e.g. partial social security numbers) or does this information need to be totally masked?
 - Section (d)(3) requires the deleting of data from archives or backup drives. This is very difficult to do, and as such, we request clarity on what is meant by “until the archived or backup system is next accessed or used.” Does this mean when data is next written to the archive or back-up, or when data is retrieved from the archive or backup?
 - Section (d)(5) requires businesses to “maintain a record of the request.” We request clarification of what this record would look like. Is it metadata around the request or is it a record of the actual retained personal information?

General Rules Regarding Verification

- Section (b)(2) states that the collecting of certain personal information should be avoided, (e.g., driver’s license) unless necessary for the purpose of verifying the consumer’s identity. We request clarity around how the necessity of collecting this information is determined. Our members require this type of information for non-account holders to verify their identity.

Exclude Probabilistic Identifiers

- We request that “probabilistic identifiers” be excluded from the definition of “unique identifier/unique personal identifier”, one of the categories of “personal information,” as these are, as their name suggests, merely predictive in nature and prone to inaccuracy. Identification of a particular consumer based on probabilistic identifiers is difficult, and businesses may find themselves inadvertently disclosing information of one consumer to another or deleting the wrong information.

Classifying “inferences drawn” as personal information

- It is currently unclear whether “personal information” includes non-public communications and content which uses or is based upon personal information, such as internally derived calculations (e.g., products and decisions generated by our member companies’ proprietary underwriting algorithms to offer capital to customers). We request that this subdivision be clarified to exclude information that is internally derived or generated and necessary for the business purpose for which the information was collected, so our member companies can continue providing the products and services sought by our small business customers.

Metadata Around a Verifiable Consumer Request Must be Retained

- When honoring a verifiable consumer request for deletion, it is essential that a business retain certain metadata from the request to document that the personal information has been properly deleted and ensure that particular customer's personal information is not re-stored in the future. If a business is not able to store such metadata, or unique identifiers or other information against which it can cross reference new data, it may inadvertently send marketing materials to a "new" customer that has previously asked to be deleted.

Additional Guidance Needed on Verifying Requests

- The CCPA allows consumers to lodge a verifiable consumer request with a business whether or not they maintain an account with the business. We request clarification on how a business is expected to verify requests from consumers that are not customers or accountholders of the business. For example, many of our members purchase marketing lists containing personal information about consumers that are candidates to receive direct mail about commercial lending products. If such a consumer submits a request to a business, the business may not be able to verify the request, as the only information the business has about the consumer is often publicly available and insufficient by itself to verify the consumer's identity. Additionally, marketing databases frequently contain inaccuracies and may be unreliable for verification. Businesses cannot comply with consumer requests without clearer guidelines on the scope of verifiable requests, as they otherwise risk sharing personal information with consumers that are unverified or not properly verified.

Timeframe for Deleting Data Upon Consumer Request

- CCPA and the proposed regulations provide for a very tight 60-day timeframe for businesses to respond to and act upon a request from a consumer to delete data. For smaller companies like ILPA members, 60 days is a very short window to respond. Unlike large internet and technology companies, our members have very limited resources to handle individual tech requests. We respectfully request expanding this timeframe to at least 90 days to give smaller businesses more flexibility to properly comply with consumer requests.

We thank you for the opportunity to present our concerns with the proposed regulations for CCPA on behalf of our members and we would be happy to meet with you at your convenience to discuss these issues as you work towards clarifying guidance.

Sincerely,



Scott Stewart, CEO
Innovative Lending Platform Association

Message

From: Alex Propes [REDACTED]
Sent: 12/6/2019 9:05:43 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Interactive Advertising Bureau Comments on Proposed CCPA Regulations
Attachments: IAB Comments on Proposed CCPA Regulations.pdf

Please find attached written comments by the Interactive Advertising Bureau in response to the proposed CCPA regulations. We appreciate this opportunity to submit these comments and if you have questions, please contact us.

Kind regards,

Alex Propes
Senior Director, Public Policy & International
Interactive Advertising Bureau
Office: [REDACTED]
Mobile: [REDACTED]



December 6, 2019

California Office of the Attorney General
ATTN: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

Submitted via privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Proposed Regulations

The Interactive Advertising Bureau (“IAB”) provides these comments on the proposed regulations issued by the California Attorney General (“AG”) on October 11, 2019 to implement the California Consumer Privacy Act (“CCPA”).

Founded in 1996 and headquartered in New York City, the IAB (www.iab.com) represents over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns. Together, our members account for 86 percent of online advertising in the United States. In California, we contribute \$168 billion to the state gross domestic product and support over 478,000 full-time jobs in the state.¹ Working with our member companies, the IAB develops technical standards and best practices and fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. The organization is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of our public policy office, the IAB advocates for our members and promotes the value of the interactive advertising industry to policymakers and legislators across the country.

The modern U.S. economy is dependent on data, and consumers derive substantial benefit from the data-driven economy. The free flow of data and information online benefits consumers by enabling access to innovative and informative content, as well as products and services, and by subsidizing the vast and varied offerings that are available to consumers through the Internet. Data-driven advertising plays a substantial role in this ecosystem by making it possible for businesses to provide low or no cost content and services to consumers through video, news, music, and much more. In fact, a recent study by Harvard Business School Professor John Deighton found that in 2016, the U.S. ad-supported Internet created 10.4 million jobs and the data-driven ad industry added 1.121 trillion to the U.S. economy, doubling its contribution over just four years and accounting for 6 percent of U.S. gross domestic product.² Other studies and surveys show that consumers are aware that online products and services are enabled by data collected about their interactions and behavior online, and they support that exchange of value. For instance, a Zogby survey commissioned by the Digital Advertising Alliance found that 85 percent of consumers surveyed stated they like the ad-supported Internet,

¹John Deighton, *The Economic Value of the Advertising-Supported Internet Ecosystem* (2017), available at <https://www.iab.com/insights/economic-value-advertising-supported-internet-ecosystem/>.

² *Id.*

and 75 percent indicated that they would greatly decrease their engagement with the Internet if another model were to take its place.³

IAB broadly supports the CCPA's, and the proposed regulations', purpose and intent to enhance consumer privacy by providing transparency and choice about the use of personal information. However, certain provisions of the proposed rules stray from or contradict the text of the CCPA itself. Other provisions, as drafted, may ultimately reduce consumer choice and undermine privacy, rather than advancing it. Finally, a few provisions set forth entirely new obligations for businesses that will be excessively burdensome to implement. IAB urges the AG to consider consumers' support for the ad-driven Internet model and asks the AG to update the proposed rules so they empower consumers by giving them increased choices and control over online data. IAB provides the following comments below, addressing specific provisions of the proposed rules that should be updated or clarified to further consumer choice and privacy and enable business compliance with the law.

I. Allow Businesses the Flexibility to Provide Effective Notices At or Before the Point of Personal Information Collection

The proposed regulations provide information about how businesses must comply with the CCPA requirement to, "at or before the point of [personal information] collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."⁴ As described in more detail below, IAB asks the AG to update the proposed regulations so they better align with the text of the CCPA and allow businesses flexibility in the mechanisms they may use to meet this requirement.

a. Clarify that notices may be visible at the time personal information is collected

The CCPA requires businesses that collect personal information to provide a notice at or before the point of collection of the categories of personal information the business collects and the purposes for which the categories are used.⁵ The proposed regulations helpfully state that businesses that collect personal information from consumers online may give such a notice by providing a link to the section of the business's privacy policy that contains the required information.⁶ However, the proposed regulations also state that the notice must "[b]e visible or accessible where consumers will see it *before any personal information is collected.*"⁷ This contradicts the CCPA, which clearly requires a notice *at or before* the point of personal information collection. We ask the AG to update this provision in the proposed regulations to reflect the statute.

In addition, the AG's draft rule does not align with common market practice online. A business typically begins collecting personal information when a consumer visits an online

³ DAA, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.

⁴ Cal. Civ. Code § 1798.100(b).

⁵ *Id.*

⁶ Cal. Code Regs. tit. 11, § 999.305(c) (proposed Oct. 11, 2019).

⁷ *Id.* at § 999.305(a)(2)(e) (emphasis added).

website, service, or mobile application owned by the business. It is therefore difficult to imagine how a business could serve a notice to a consumer before the point of personal information collection. As such, we ask the AG to modify Section 999.305(a)(2)(e) of the draft regulations to clarify that notice at or before the point of collection must be visible *at the time of* or before any personal information is collected. This update would bring the proposed regulations into conformity with the CCPA’s text and better reflect what is possible given the realities of the online data-driven ecosystem.

- b. *Clarify that businesses may make new uses of collected personal information by providing notice of the new use to the consumer*

The CCPA states that a business may not “collect additional categories of personal information or use personal information collected for additional purposes [other than those identified in the notice at collection] without providing the consumer with notice” of such new categories of personal information or additional purposes.⁸ However, the proposed regulations state that “[i]f the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use *and obtain explicit consent* from the consumer to use it for this new purpose.”⁹ This “explicit consent” requirement in the proposed regulations does not align with the CCPA’s text, which focuses exclusively on notice to the consumer and does not refer to explicit consent. This point is further supported by the CCPA’s definition of one of the exceptions to the “sale” definition where a third party assumes control of a business and makes a material change to the privacy policy, noting a prominent notice requirement, but not mentioning a consent requirement.¹⁰ We ask the AG remove the following language “*and obtain explicit consent* from the consumer to use it for this new purpose” as it exceeds the scope of the CCPA’s statutory language.

The requirement to obtain “explicit consent” for a new use of personal information moves beyond the CCPA’s text and imposes a substantial requirement on businesses that was not intended by the California legislature when it considered and passed the CCPA. Such a requirement also would lead to an inconsistency in the CCPA requirements on when new data use occurs by a business versus a third party that assumes control of a business. Furthermore, this provision of the proposed regulations is clearly outside of the scope of the CCPA, as the law itself only requires businesses to notify consumers of a new use of data and does not require “explicit consent.” IAB therefore asks the AG to revise the proposed regulation in line with the CCPA’s text and remove the proposed requirement that businesses need to obtain “explicit consent” for such new uses.

- c. *Allow third parties to rely on attestations from data suppliers stating that consumers were given notice and choice consistent with the CCPA*

According to the proposed regulations, although a business that does not collect information directly from consumers does not need to provide a notice at collection, such a

⁸ Cal. Civ. Code § 1798.100(b).

⁹ Cal. Code Regs. tit. 11, § 999.305(a)(3) (proposed Oct. 11, 2019) (emphasis added).

¹⁰ Cal. Civ. Code § 1798.140(t)(2)(D).

business must take certain specific actions before selling personal information.¹¹ Before selling personal information, a business that does not collect information directly from consumers must either: (1) contact the consumer to provide notice of sale and notice of the right to opt-out of sale, or (2) confirm that the source provided a notice at collection, obtain signed attestations describing how the source provided such a notice, obtain an example of the notice, retain the attestations and example notices for at least two years, and make them available to consumers upon request.¹² IAB asks the AG to amend the proposed regulations so that businesses may rely on signed attestations from their immediate data suppliers that the consumer was given notice of personal information sale and an opportunity to opt-out only, and need not obtain samples of the notices that were provided to consumers, retain them, or make them available to consumers upon request. IAB also asks the AG to confirm that the attestations companies receive, and the example notices they may be required to maintain do not need to be returned to consumers in response to CCPA access requests.

Allowing entities to obtain contractual representations from their immediate data suppliers that the consumer was notified of personal information sale and the right to opt-out of such sale provides the same consumer benefits as requiring businesses to maintain an example of the notice that was actually provided to the consumer. The requirement to retain examples of the notice provided to consumers and to make them available at a consumer's request is unmanageable for businesses, as they could have to maintain thousands if not millions of notices. For example, in the programmatic advertising context where billions of data exchanges occur on a second-by-second basis, businesses would have no reasonable way to pass model notices to entities in the ecosystem that receive data. In addition, this provision could be interpreted to require businesses to pass example notices down the chain from the original source of data to other businesses who may receive personal information, which is an unrealistic and potentially impossible burden for businesses to meet. Consumers receive little if any additional benefits from the example notice requirement, as consumers receive the same level of transparency and choice through requiring businesses to obtain attestations that consumers were given such notices. Moreover, requiring businesses to obtain examples of the consumer notices that were provided and retain this information for two years would require companies to amend agreements that have recently been amended under prior interpretations of the CCPA.

In addition, IAB urges the AG to update the proposed rules so that businesses are not obligated to return the sample notices they may be required to maintain or the attestations they receive from data sources to consumers in response to access requests. The California legislature determined that businesses are not required to disclose particular data sources to consumers in response to access requests by expressly stating that the access right requires the disclosure of categories of sources of personal information and not the particular data sources themselves. In addition, a requirement to return attestations and sample notices to consumers in response to an access request runs the risk of exposing confidential or proprietary business terms to the public. Moreover, in a practical sense, it is unworkable for businesses to have to link individual data points to consumers and contractual terms.

¹¹ Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).

¹² *Id.*

IAB asks the AG to clarify that businesses may rely on signed attestations from their immediate data suppliers that the consumer was given notice of the personal information sale and an opportunity to opt-out. IAB also asks the AG to clarify that a business is not required to produce the attestations it receives from data sources or sample notices it may be required to maintain to a consumer in response to an access request.

To provide clarity on additional business cases, we would also ask that the AG clarify that a third party, without knowledge of presentation of an opt-out, may present the opt-out opportunity to the consumer, so long as the consumer has adequate notice of the third party's collection of the data at the time of collection. In this way, a third party may provide the opt-out service to its customers' consumers who are in the position of direct collection.

II. Remove the Requirement to Provide an Estimate of the Value of Consumer Data and the Method of Calculating the Value of Consumer Data in a Notice of Financial Incentive

If a business offers a financial incentive or a price or service difference to a consumer in exchange for the retention or sale of personal information, the proposed regulations require the business to provide a notice to the consumer that includes: (1) 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 (2) a description of the method the business used to calculate the value of the consumer's data.¹³ IAB respectfully asks the AG to remove the requirement to provide an estimate of the value of the consumer's data and the method of calculating such value, as these obligations are not contemplated by the CCPA itself, would be difficult if not impossible for a business to provide, and could potentially reveal confidential or proprietary information about the business's internal practices and economic assessments.

First and foremost, the requirement to provide an estimate of the value of the consumer's data and the method of calculating such data is extralegal. These provisions of the proposed regulations represent brand new business obligations that were not included in the text of the CCPA itself. Businesses have spent over a year preparing for the CCPA's effective date of January 1, 2020. Adding substantial and disruptive new requirements to the CCPA, such as these requirements related to financial incentives, less than three months before the law will go into effect causes significant compliance complications and challenges for businesses of all sizes.

Second, it may be impossible for businesses to comply with the requirement to provide an estimate of the value of the consumer's data, because data lacks clear, objective value. Academics have come up with wildly different estimates for the value of data-enabled services,¹⁴ and experts are likely to come up with differing values for these services in the future as well.

Finally, the requirement to provide an estimate of the value of the consumer's data and the method for computing such value could expose confidential, proprietary business information

¹³ *Id.* at § 999.307(b)(5).

¹⁴ Asha Saxena, *What is Data Value and should it be Viewed as a Corporate Asset?* (2019), located at <https://www.dataversity.net/what-is-data-value-and-should-it-be-viewed-as-a-corporate-asset>.

or put a business's competitive position at risk.¹⁵ Despite the challenges of estimating the value of the consumer's data, the method by which a business values personal information associated with a consumer in order to comply with their obligations under the proposed rule may constitute proprietary information about the business's commercial practices. Forcing businesses to reveal such confidential, secret information could harm businesses' ability to compete in the marketplace, as competitors and customers would become aware of the value a business has assigned to the data it maintains. Obligating businesses by law to reveal this information could harm the economy and healthy business competition by forcing companies to reveal confidential information.

For the foregoing reasons, IAB asks the AG to remove the proposed regulations' requirement that a business must, in a notice of financial incentive, provide an estimate of the value of the consumer's data and the method by which it calculated such value. This directive constitutes a requirement that goes far beyond the requirements of the CCPA itself. Furthermore, the requirement could be impossible for businesses to effectuate and would risk distorting business competition.

III. Ensure Requirements for Requests to Know and Delete Align with the CCPA's Text, Consider Real-World Implications, and Empower Consumer Choice

Certain provisions in the proposed regulations set forth rules about consumer requests to know and requests to delete that do not align with the CCPA, and other portions of the proposed regulations fail to consider significant real-world outcomes associated with their requirements. Finally, some of the provisions thwart consumers' ability to make choices and require businesses to take action on personal information in ways that may not be approved by the consumer. IAB requests that the AG update the proposed rules, as further described below, to conform them with the CCPA's text, better align them with practical realities, and empower consumers to make meaningful choices that businesses must respect.

- a. *Consistent with the text of the CCPA, enable businesses that have direct consumer relationships and operate exclusively online to provide an email address only for consumers to submit CCPA requests to know*

The CCPA, as recently amended by California AB 1564,¹⁶ states that “[a] business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.”¹⁷ However, the proposed regulations state that “[a] business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's

¹⁵ IAB also respectfully disagrees with the AG's assessment that providing consumers with these calculations will provide meaningful information about the costs and benefits of the financial incentive to the consumer specifically. *See* Initial Statement of Reasons at 12. The calculations described in the proposed regulation reflect the value proposition to the business, not to the consumer.

¹⁶ AB 1564 (Cal. 2019).

¹⁷ Cal. Civ. Code §§ 1798.105(a), (c).

website or mobile application.”¹⁸ The CCPA and proposed regulations are therefore directly at odds, as the CCPA requires businesses with direct consumer relationships that operate exclusively online to provide an email address only for consumers to submit requests to know, while the proposed regulations require a toll-free number and an interactive webform for businesses to receive such requests. IAB asks the AG to conform the proposed regulations to the text of the CCPA and clarify that businesses who maintain direct relationships with consumers and operate exclusively online must provide only an email address or webform for receiving consumer requests to know.

- b. *Extend the time period within which businesses must confirm receipt of a request to know or delete and provide information about how the business will process the request*

The proposed regulations state that “upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 days and provide information about how the business will process the request.”¹⁹ This requirement is impractical for businesses, as it provides insufficient time for a business to decide how it will process a request. Ten days does not allow enough time for a business to fully vet a request, verify the identity of the requestor, ascertain whether it must avail itself of a permitted exception to fulfilling the request, or take any other due diligence steps necessary to be able to provide an accurate description of how it will process the request to the consumer. IAB therefore asks the AG to extend the time period within which businesses must confirm receipt of a request to know or a request to delete and provide information about how it will process a request. IAB suggests the AG extend the period to thirty days, which is a time period within which businesses must comply with consumer requests under other privacy regimes, such as the General Data Protection Regulation.

Furthermore, we ask that a business’s request for information to verify a consumer’s identity before effectuating a consumer request tolls or pauses the 45-day window within which the business must respond to the request. Consumer verification is necessary for businesses to accurately effectuate consumers’ CCPA rights. Robust and accurate verification is in the interest of consumers, because without it, businesses run the risk of erasing or returning data that does not pertain to the requesting consumer.

- c. *Confirm that businesses need not delete personal information if maintaining it is necessary to provide expected subscription messages*

The CCPA requires businesses to delete “any personal information about the consumer which the business has collected from the consumer” upon receipt of a verifiable consumer request.²⁰ The law exempts businesses from the need to delete personal information if maintaining it is necessary for the business to “provide a good or service... reasonably anticipated within the context of a business’s ongoing business relationship with the consumer, or otherwise perform a contract with the consumer,”²¹ but it does not explain what conduct can

¹⁸ Cal. Code Regs. tit. 11, § 999.312(a) (proposed Oct. 11, 2019).

¹⁹ *Id.* at § 999.313(a).

²⁰ Cal. Civ. Code §§ 1798.105(a), (c).

²¹ *Id.* at § 1798.105(d)(1).

be considered “reasonably anticipated” within an “ongoing business relationship” with a consumer. IAB asks the AG to clarify this CCPA exception to the deletion right so that businesses may continue to provide expected subscription messages to consumers that are reasonably anticipated within the context of the business’s ongoing relationship with a consumer.

We urge the AG to clarify what is “reasonably anticipated within the context of a business’s ongoing business relationship with the consumer.” Such a regulation should explicitly confirm that expected subscription messages are reasonably anticipated within an ongoing business relationship with a consumer that maintains a subscription with the company following a deletion request. If a consumer maintains a subscription with a company after requesting that the company delete the consumer’s personal information, it is reasonable for the company to assume the consumer did not mean to cancel his or her subscription. As such, the AG should clarify that requests to delete personal information do not require businesses to delete information they would need to provide consumers with messages they expect to receive during the course of a subscription arrangement with a business. Such a rule would advance consumer privacy by reducing uncertainty around the kinds of data businesses must delete in response to a verifiable request. It would also provide further clarity for businesses with respect to their obligations under federal privacy laws on direct marketing.

d. *Remove the requirement to treat deletion requests as requests to opt-out of the sale of personal information if a requestor’s identity cannot be verified*

Per the proposed regulations, if a business cannot verify the identity of a requestor who has submitted a request to delete, the business may deny the request to delete.²² The business must then “inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.”²³ This requirement essentially forces businesses to act in ways that may not align with consumer choices or preferences. A consumer request to delete personal information does not mean that the consumer would agree to the business transforming that request into a request to opt-out of the sale of personal information. Furthermore, the requirement to transform unverifiable requests to delete into requests to opt-out of personal information sale ignores the fact that if a business cannot verify a consumer request, it may not be able to associate the requestor with any personal information to opt-out from sale. As such, IAB asks the AG to reconsider the requirement to act on unverifiable requests to delete as if they are requests to opt-out of personal information sale, as this mandate does not honor consumer preferences or acknowledge practical realities associated with unverifiable consumer requests.

The AG’s proposed rule requiring businesses to pass opt-outs to third parties to whom they have sold personal information in the past 90 days would mean that unverified deletion requests that are converted into opt-out requests could have extremely broad and far-reaching implications for consumers. This result may not align with a consumer’s expectation when submitting a request to delete. While a request to delete has effects for the business that receives the request, a request to opt-out has effects for third parties and the consumer, as third parties who receive consumer data may be providing consumers with products and services. If, as suggested in the Initial Statement of Reasons, the AG’s goal is to “at least [prevent] the further

²² Cal. Code Regs. tit. 11, § 999.313(d)(1) (proposed Oct. 11, 2019).

²³ *Id.*

proliferation of the consumer’s personal information in the marketplace,” this can be solved through directing the consumer to opt-out of the sale of their personal information in correspondence with the consumer.²⁴ Otherwise, transforming consumer requests to delete into requests to opt-out if a request cannot be verified runs the risk of thwarting consumer choice and forcing businesses to act in ways that do not align with a consumer’s wishes.

In addition, if a business cannot verify a consumer request to delete, the business may not be able to associate that consumer with any personal information it maintains in order to facilitate an opt-out. If a business cannot verify a consumer, it cannot ascertain that the consumer making the request is a consumer about whom it maintains personal information in its systems. As such, the lack of verification presents a challenge for businesses in their efforts to effectuate both consumer requests to delete *and* requests to opt-out, as businesses must achieve a certain level of consumer verification for both requests to ensure they are acting on the correct consumer’s data in their systems. As a result, the proposed regulations’ requirement that businesses transform unverifiable consumer requests to delete into requests to opt-out of personal information sale does not take into account that the lack of verification could thwart the business’s ability to opt the consumer out from personal information sale just as it thwarts the business’s ability to delete consumer personal information.

Because the requirement to turn unverifiable requests to delete into requests to opt-out of personal information sale could contradict consumer preferences, and because businesses will have the same difficulties effectuating unverified requests to opt-out as they will unverified requests to delete, IAB asks the AG to reconsider the provision that requires businesses to transform unverified requests to delete into requests to opt-out. Removing this requirement from the proposed regulations will ensure that consumer choices are not hindered by businesses taking unilateral actions to transform their requests.

e. *Retain the deletion exception for archival and backup systems and the ability for businesses to present consumers with granular deletion choices*

The proposed regulations helpfully clarify that a business can comply with a consumer’s request to delete by “erasing the personal information on its systems *with the exception of archived or back-up systems.*”²⁵ IAB appreciates the AG’s recognition of the challenges associated with fulfilling consumer requests as they relate to data in archival and backup systems. As IAB highlighted in its pre-rulemaking comments to the AG in March, if consumer requests can reach data held on backup or archival systems, the costs associated with these requests would be excessive. In addition, if deletion requests were required to reach such systems, businesses’ ability to rebound from data failures and comply with legal obligations would be severely limited.

However, the proposed regulations state that a business “may delay compliance with [a] consumer’s request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used.” While IAB supports the AG’s consideration of the challenges associated with data deletion in certain storage scenarios, we

²⁴ See Initial Statement of Reasons at 20.

²⁵ *Id.* at § 999.313(d)(3).

recommend that archived and backup systems be fully exempted from consumer deletion requests by removing the proposed obligations that apply when archived and backup systems are next accessed or used.²⁶

In addition, the proposed regulations note that “[i]n responding to a request to delete, a business may present the consumer with the choice to delete select portions of the personal information only if a global option to delete all personal information is also offered, and more prominently presented than the other choices.”²⁷ IAB supports this provision, as it gives consumers the ability to delete granular pieces of personal information and does not force them to make all-or-nothing choices when it comes to personal information deletion. IAB recommends retaining this option when the AG finalizes its rules implementing the CCPA.

f. Clarify that a business may provide only the data “as of” the date of the request instead of “as of” the date of the disclosure

Businesses with large amounts of data to query to fulfill the consumer’s data request cannot practically query their data and render it in real time. If the data is gathered that is on hand on the date the consumer makes the request and any new data would be similar, the consumer has received the transparency contemplated by the law. The AG should permit this to allow different types of businesses the ability to comply with the law.

IV. Update the Service Provider Limitations to Conform with Permissible Business Purposes Enumerated in the CCPA

The proposed regulations state that “[a] service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity.”²⁸ This language is qualified by two exceptions: “A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.”²⁹ Taken together, these provisions could be read to prohibit service providers from using data for the full range of internal operations purposes for which they are permitted to use it under the CCPA. As such, IAB requests that the AG revise these proposed rules to reflect that using personal information received from a person or entity a service provider services for the purpose of providing services to another person or entity is a permissible “business purpose” under the CCPA. This change could be accomplished by adding an additional exception for a service provider “to perform services that fulfill a business purpose, so long as such use is for the benefit of the business, is described in the written contract between the business and service provider, and is consistent with the CCPA.”

The draft regulations limit service providers’ permissible uses of data in ways that contradict the statutory definitions of “service provider” and “business purpose.” The text of the CCPA explicitly permits disclosures to “service providers” for a list of enumerated “business

²⁶ Cal. Code Regs. tit. 11, § 999.313(d)(3) (proposed Oct. 11, 2019).

²⁷ *Id.* at § 999.313(d)(7).

²⁸ *Id.* at § 999.314(c).

²⁹ *Id.*

purposes” under the statute.³⁰ The statute then defines “business purpose” to include *both* a business’s *or a service provider’s* operational purposes or other notified purposes.³¹ As such, so long as a permissible service provider “business purpose” is authorized as part of the contracted-for “services” provided to the business, the CCPA permits a service provider to use the personal information it receives for such a business purpose.

Because a service provider’s business purposes may include using personal information for the benefit of one business in a way that may also benefit other businesses, the CCPA is best interpreted to permit a service provider to use personal information it receives to provide services to all of its business partners, as long as such use is for the benefit of the business that provides the information to the service provider, is performed for a valid business purpose, and is otherwise consistent with the CCPA. However, the proposed regulations depart from the CCPA text, as they seem to prohibit service providers from using personal information they receive from one entity to provide services to another entity, even if such use stands to benefit the business that provided the personal information to the service provider for a business purpose.

Moreover, the draft regulations improperly read out of the statute that the definition of “business purpose” includes the use of personal information for the “service provider’s operational purposes or other notified purposes.”³² The activities included in the list of business purposes (*i.e.*, performing services on behalf of the business or service provider, including providing advertising or marketing services, providing analytic services, or providing similar services) require the combination and use of personal information received from and for the benefit of multiple businesses. Focusing solely on the business purposes of the business renders the CCPA’s text meaningless, and potentially invalidates several activities included in the definition of permissible business purposes under the law. As such, IAB asks the AG to clarify that a service provider may use personal information if the usage is within the scope of a “business purpose” as authorized as part of the contracted-for “services” provided to the business, or necessary for the service provider’s own operational purposes and is otherwise consistent with the requirements of the CCPA.

Importantly, if the AG were to maintain the proposed restrictions on service providers, the AG has not conducted an adequate standardized regulatory impact analysis (“SRIA”).³³ The SRIA submitted with the draft regulations is entirely silent on the likely detrimental impact of restricting service providers from performing services for a business purpose.³⁴ As a result, the SRIA fails to consider possible “elimination of existing businesses within the state” or “competitive ... disadvantages for businesses currently doing business within the state,” falling far short of the mandatory analysis required by the California Administrative Procedure Act.³⁵

³⁰ Cal. Civ. Code §§ 1798.140(d), (v).

³¹ *Id.* at § 1798.140(d).

³² *Id.*

³³ See Cal. Gov. Code § 11346.3(c).

³⁴ See Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations (Aug. 2019), at 17 (hereinafter “SRIA”) (concluding with regard to the draft regulations pertaining to service providers, “all other economic impacts associated with language in Article 3 are assumed to be attributable to the CCPA and are therefore included in the regulatory baseline.”).

³⁵ Cal. Gov. Code § 11346.3(c)(1)(B), (C).

V. The AG Should Confirm That Section 999.314(c) Does Not Limit Businesses from Collectively Engaging Service Providers to Conduct Necessary Operational Activities Pursuant to “Business Purposes”

Additionally, upon IAB’s review of Section 999.314(c), we do not see that it applies to or otherwise conflicts with the ability of multiple “businesses” that have collectively engaged service providers through the same contract or otherwise to conduct certain operational activities pursuant to “business purposes” that involve the combination of personal information. In such circumstances, Section 999.314(c) does not apply because these activities fulfill the “commercial purposes” of the contracting businesses, rather than serve the “commercial purposes” of the service providers. While we see no conflict with the existing language in such circumstance, IAB respectfully requests that the following clarifying language be added to Section 999.314(c):

Notwithstanding the above restrictions, service providers that are engaged jointly or collectively on behalf of two or more businesses to fulfill necessary business purposes can combine, use, and share personal information as long as such activities are consistent with the commercial purposes of the businesses rather than the commercial purposes of the service providers.

This clarification is consistent with the express language of the CCPA permitting service providers to use personal information for operational and permitted business purposes,³⁶ and supports the CCPA’s privacy objectives to restrict a service provider from using personal information for its own “commercial purposes.”³⁷ The clarification also satisfies the underlying goal stated in the Initial Statement of Reasons to prevent advancing the “commercial interest” of the service provider, rather than fulfilling the contracted “business purpose.”³⁸

The impetus for this clarification is the prevalence of joint engagements, operations or co-venture business models that hire service providers to support their joint activities. For example, companies may offer co-branded services wherein two companies provide a single offering to consumers. Similarly, businesses may enter into a joint agreement to provide a consistent user experience across digital platforms, devices, or internet domains. In these examples, the businesses require the ability to contract with a common set of service providers that, on behalf of the businesses, use personal information to support the businesses’ operations (*i.e.*, the businesses’ commercial purposes for providing the services).

For these reasons and to avoid any confusion or unnecessary disruption of multiple industries that rely on service providers to work jointly to assist a business, IAB urges the AG to clarify that Section 999.314(c) does not prohibit businesses from collectively engaging service providers to perform operations necessary for the businesses’ commercial purposes, such as in joint or co-venture arrangements.

³⁶ Cal. Civ. Code §§ 1798.140(d), (v).

³⁷ See Cal. Civ. Code § 1798.140(v).

³⁸ Initial Statement of Reasons at 22.

VI. Consumer Opt-Outs Should Empower Consumers

IAB recommends that the AG make changes to the draft regulations' provisions related to opt-out requests so that they conform with the CCPA's text, as requirements that are not supported by the law's text do not further the California legislature's intent in enacting the CCPA.

- a. *Requiring businesses to honor browser plugins or settings goes beyond the scope of the CCPA and creates significant compliance challenges that could impede consumer choice*

The proposed regulations state that “[i]f a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy 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... for that browser or device, or, if known, for the consumer.”³⁹ This proposed regulation exceeds the CCPA’s scope, imposing new substantive requirements on businesses that the legislature has previously considered and elected to not include.⁴⁰ We request that the AG remove this requirement, or alternatively, where a business offers a “Do Not Sell My Info” link and a means to opt-out from sale, the business is not required to treat the proposed controls as an opt-out. Such an approach would be consistent with the approach taken by the legislature when it amended the California Online Privacy Protection Act.

At this juncture, it would be premature to regulate in this area or mandate that every business comply with each type of signal developed to facilitate CCPA compliance. Given that no standard technology currently exists for such browser plugins or privacy settings, it is not clear what browser plugins or privacy signals should be honored or how they should be honored. Absent standard technical and policy protocols around how to honor such signals, the proposed regulations would give rise to different signals and interpretations and result in confusion among businesses and consumers alike.

The AG takes the position that in the absence of mandatory support for privacy controls, “businesses are likely to reject or ignore consumer tools.”⁴¹ As the CCPA comes into effect in 2020, IAB expects to see market forces leading to strong demand for compliance solutions that can facilitate both consumer choice and business compliance. Throughout the online ecosystem, IAB also expects to see consumers take advantage of multiple compliance solutions, informed by privacy notices directing consumers on how to communicate their privacy choices.

If the AG chooses to maintain this requirement, we suggest that the AG alter it so that a business engaged in the sale of personal information must *either* abide by browser plugins or privacy settings or mechanisms, or may not honor such settings if the business includes a “Do Not Sell My Personal Information” link and offers another method for consumers to opt-out of personal information sale by the business. This approach affords consumers with robust choice and control over the sale of personal information. Browser-based signals or plugins would

⁴⁰ See [CalOPPA & September 2018, 2019 amendments to CCPA]

⁴¹ See Initial Statement of Reasons at 24.

broadcast a single signal to all businesses opting-out a consumer from the entire data marketplace. It is not possible through these settings for a consumer to make discrete choices among businesses allowing the consumer to restrict certain businesses while permitting other businesses to transfer data to benefit the consumer. In addition, it is not possible for a business to verify if a consumer set the browser setting or some intermediary did so without the authorization of the consumer.

- b. *Remove the requirement to communicate opt-out requests to third parties that received the consumer's personal information within the prior ninety days*

As noted above in Section III(d), the proposed regulations require a business that receives an opt-out request to notify all third parties to whom it has sold personal information about the consumer making the opt-out in the past 90 days prior to the request that the consumer has opted out and instruct those third parties not to further sell the information.⁴² IAB asks the AG to withdraw this proposal because it has no basis in the CCPA's statutory text and would result in negative consequences for consumers by amplifying, without a reasonable basis, the consumer's opt-out request aimed at just one business.

The proposed rule is not supported by the CCPA's text and goes beyond the proper scope of the AG's rulemaking authority. The CCPA states that a consumer has "the right, at any time, to direct *a business* that sells personal information about the consumer to third parties not to sell the consumer's personal information."⁴³ The plain language of the statute makes clear that the legislature intended the opt-out to apply to businesses only and did not grant consumers an opt-out right vis-a-vis third parties to whom personal information was already sold. Had the legislature intended the opt-out to have retroactive application to already sold personal information, it would have done so in the statute.⁴⁴

The proposed rule also fundamentally changes the careful balancing of privacy rights with burdens on businesses, which the legislature decided upon with the CCPA. Indeed, the definition of a "sale" indicates the sale takes place for "monetary or other valuable consideration." Obligating a business to later restrict a recipient from further selling personal information is a material retroactive change to the basis of the bargain upon which the personal information was "sold" for consideration. If the draft regulations impose obligations on the seller and buyer after the sale, the seller and buyer will essentially be required to agree to a contingent transfer subject to the receipt of do not sell requests. This contingency will impact the value of the personal information sold and the underlying consideration of the transaction. The legislature did not contemplate such an outcome.

Additionally, the CCPA is structured in a manner that makes clear the legislature's intent that the opt-out applies to businesses and not to third parties. The CCPA only once refers to

⁴² Cal. Code Regs. tit. 11, § 999.315(f) (proposed Oct. 11, 2019).

⁴³ Cal. Civ. Code § 1798.120(a).

⁴⁴ See *W. Sec Bank v. Super. Ct.*, 933 P.2d 507, 513 (Cal. 1997) (statutes will not "operate retrospectively unless the Legislature plainly intended them to do so."); see also *Myers v. Philip Morris Cos., Inc.*, 50 P.3d 751, 759 (2002) ("unless there is an express retroactivity provision, a statute will *not* be applied retroactively unless it is *very clear* from extrinsic sources that the Legislature . . . must have intended a retroactive application" (citations and quotation marks omitted; emphases in original)).

third party obligations regarding the handling of personal information that has been sold to the third party.⁴⁵ Otherwise, the CCPA focuses entirely on the obligations of businesses to provide the right to opt-out.⁴⁶ Through this emphasis on the obligations of businesses, the CCPA favors letting consumers make an opt-out choice up front before the personal information flows to third parties.⁴⁷

The draft regulations are invalid to the extent that they exceed the scope of the AG's statutory authority⁴⁸ or read into the statute additional requirements that go beyond the statutory scheme of the CCPA.⁴⁹ It is true that the CCPA provides the AG with the ability to establish rules and procedures "to govern business compliance with a consumer's opt-out request."⁵⁰ However, that provision does not vest the AG with the authority to write rules that extend the scope of the opt-out beyond the plain language and clear intent of the statute such that the opt-out retroactively applies to third parties.⁵¹

In addition, the draft regulation will likely lead to consumer confusion around the meaning of the opt-out of sale request, with damaging economic effects. The proposal assumes that a consumer's desire to opt-out of one business's sale of personal information represents a request that the consumer would like to have this request applied retroactively to third parties to whom their personal information was already sold. It is not clear that a consumer would expect an opt-out of sale button to operate in this manner, and indeed, the consumer's actual intentions may be frustrated if the AG were to draw such an unfounded conclusion. Furthermore, obligating businesses to pass opt-out requests on to third parties and to instruct those third parties not to further sell information could have damaging effects on the Internet economy, as the free flow of data that powers the Internet will be stifled by a consumer expressing an opt-out choice aimed at one business only.⁵² Consumers will receive fewer digital offerings and decreased access to products and services that interest them if this requirement becomes effective.

⁴⁵ See Cal. Civ. Code § 1798.115(d).

⁴⁶ See Cal. Civ. Code § 1798.120.

⁴⁷ See Cal. Civ. Code § 1798.120(b).

⁴⁸ See *In re J.G.*, 159 Cal. App. 4th 1056, 1066 (2008) (invalidating correction department regulation which exceeded statutory authority).

⁴⁹ See *Slocum v. State Bd. of Equalization*, 134 Cal. App. 4th 969, 981 (2005) (invalidating State Board of Equalization interpretative regulation because it acted to provide more relief than statutorily authorized); see also *Sabatasso v. Superior Court*, 167 Cal. App. 4th 791, 797 (2008) (invalidating penal regulation which went beyond scope of delineated statutory authority).

⁵⁰ Cal. Civ. Code § 1798.185(a)(4)(B).

⁵¹ See *Home Depot, U.S.A., Inc. v. Contractors' State License Bd.*, 41 Cal. App. 4th 1592, 1600, 49 Cal. Rptr. 2d 302, 306 (1996) ("A regulation cannot restrict or enlarge the scope of a statute" (citing Cal. Gov. Code §§ 11342.1, 11342.2).); *Ontario Cmty. Foundations, Inc. v. State Bd. of Equalization*, 35 Cal. 3d 811, 816, 678 P.2d 378, 381 (1984) ("[T]here is no agency discretion to promulgate a regulation which is inconsistent with the governing statute.").

⁵² The SRIA is also deficient on this point. See SRIA at 25-26. The SRIA indicates "[t]he incremental compliance cost associated with this regulation is the extra work required by businesses to notify third parties that further sale is not permissible." *Id.* at 25. This comment overlooks the ripple effect as the opt-out of sale request will restrict uses of personal information including those generally occurring subsequent to the sale transaction. The SRIA should consider how restricting the sale of personal information by third parties in this way can "increase or decrease ... investment in the state." Cal. Gov. Code § 11346.3(c)(1)(D).

Because the requirement to pass opt-out requests along to third parties is outside the scope of the CCPA and because of the negative effects such a requirement will have on consumers and the Internet economy alike, IAB asks the AG to remove this requirement from the proposed regulations. Doing so will help the CCPA better align with legislative intent and will stop the law from harming consumers by decreasing their ability to benefit from increased access to online products and services.

VII. Provide Additional Flexibility for the Two-Step Requirement for Opting-In to the Sale of Personal Information

Per the proposed rules, if a consumer wishes to opt-in to the sale of personal information after previously opting-out of such sale, the consumer must undertake a two-step process to confirm their choice to opt-in.⁵³ “Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.”⁵⁴ This two-step requirement creates unnecessary friction in the user experience and makes it more difficult for businesses to take action to effectuate a consumer’s valid choice to opt-in to personal information sale. Businesses should be able to accept a consumer’s single communication of a desire to opt-in to personal information sale as a legitimate consumer preference and should be able to act on that validly communicated consumer choice. IAB therefore requests that the AG reconsider this requirement and provide additional flexibility for businesses and consumers for requests to opt-in to personal information sale after previously opting-out.

VIII. Clarify that Businesses Need Not Keep Records About Opt-Out Requests Served on Other Businesses

The proposed regulations require all businesses to “maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.”⁵⁵ This requirement creates compliance challenges for businesses when it comes to retaining records about consumer opt-out requests depending on the actual entity that is effectuating the opt-out. For example, in many situations in the online Internet ecosystem, first-party publisher businesses may not have any control over or the ability to know how a third-party business responds to a consumer’s opt-out choice. IAB therefore asks the AG to clarify that businesses only must keep records about the opt-out requests they receive directly from consumers and the actions the business itself took to respond to those requests and need not maintain information about other businesses’ responses to consumer opt-out requests.

IX. Clarify the Household Concept

The CCPA gives consumers the right to access personal information, and the law’s definition of personal information includes “household” data.⁵⁶ The proposed regulations define “household” to mean “a person or group of people occupying a single dwelling.”⁵⁷ Moreover,

⁵³ Cal. Code Regs. tit. 11, § 999.316(a) (proposed Oct. 11, 2019).

⁵⁴ *Id.*

⁵⁵ *Id.* at § 999.317(b).

⁵⁶ Cal Civ. Code § 1798.140(o)(1).

⁵⁷ Cal. Code Regs. tit. 11, § 999.301(h).

per the proposed rules, if a consumer does not maintain a password protected account with a business, the business may respond to that consumer’s request to know “household personal information” by providing “aggregate household information” so long as the requestor has been verified in accordance with the proposed regulations.⁵⁸ And if all consumers in a household jointly request to know “specific pieces of personal information for the household” or delete household personal information, the business must comply with the request if all the household members have been verified.⁵⁹ IAB asks the AG to clarify the household concept and provide instructions on how businesses can reasonably comply with the requirement to return household data in response to a consumer access request.

Returning household data to a requesting consumer or consumers creates privacy concerns, because a business might provide a consumer’s personal information to a household member who should not have access to such data, creating the potential for a data leakage facilitated by a legal obligation. In addition, returning “aggregate” data to a single consumer requesting information about a household could still reveal private information about another member of the household. For example, if a business maintains information in the aggregate about a household income, returning that information in response to a single consumer’s request could present income information about other members of the household to the requesting consumer. IAB therefore asks the AG to clarify how businesses can comply with the requirement to return household data, especially when doing so could reveal private or sensitive information about other members of the household.

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the AG on developing final regulations to interpret the CCPA. If you have questions, please contact us.

Respectfully submitted,

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

Michael Hahn
Senior Vice President & General Counsel
Interactive Advertising Bureau
[REDACTED]

⁵⁸ *Id.* at § 999.318(a).

⁵⁹ *Id.* at § 999.318(b).

Message

From: Kevin McKinley ([REDACTED])
Sent: 12/6/2019 11:29:46 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Internet Association Comments on California Consumer Privacy Act of 2018 Proposed Regulations
Attachments: IA Comments on CCPA Proposed AG Regulations.pdf

Privacy Regulations Coordinator:

I have attached Internet Association comments on the proposed CCPA Regulations.

Thank you,

--



Kevin McKinley

Director, California Government Affairs

O: [REDACTED]
[REDACTED]

INTERNET ASSOCIATION

1303 J Street, Suite 400, Sacramento, CA 95814



December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
Via email: privacyregulations@doj.ca.gov
Re: Internet Association Comments on California Consumer Privacy Act of 2018 Proposed Regulations

To Whom It May Concern:

Internet Association (“IA”) appreciates the opportunity to provide the Attorney General’s Office (“AGO”) feedback on the Text of Proposed Regulations for the California Consumer Privacy Act (“CCPA”) Regulations (“Proposed 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. It is essential that the U.S. enact a comprehensive, federal privacy law that provides Americans consistent protections and controls regardless of where they live, work, or travel.

As expressed in IA’s comments submitted to the Attorney General during the drafting period for these regulations,³ IA hoped that the AGO would use the regulations as an opportunity to clarify the CCPA in ways that would promote strong consumer privacy protections and businesses’ ability to comply with the statute’s legal requirements. IA is concerned that the proposed regulations place confusing and unnecessary burdens on businesses without providing meaningful privacy protections for consumers. The Proposed Regulations require significant new actions that go beyond the Legislature’s original intent for CCPA. It will result in a confusing barrage of notices and disclosures that frustrate consumers and fail to provide stronger protections. Modern privacy controls emphasize contextual cues to help consumers make real time decisions about how their information is used. The Proposed Regulations

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_full-doc/ (last accessed November 25, 2019).

³ IA Comments on CCPA Initial Rulemaking begin at p. 857 of the CCPA Public Comments available at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf> (last accessed November 25, 2019).



represent a leap backwards with new disclosure and notice requirements that don't provide consumers strong protections or controls and harm businesses.

IA urges the AGO to use the remaining time available to amend the regulations in a manner consistent with the CCPA's provisions and that facilitates implementation and compliance with its terms.

Section I. General Comments

IA would like to share a few high level concerns that apply to the Proposed Regulations as a whole, before providing our comments on specific provisions:

1. The Proposed Regulations introduce new requirements too close to the effective date of CCPA.

The CCPA's provisions become operative on January 1, 2020 pursuant to Cal. Civil Code Section 1798.198(a). The Attorney General is able to bring enforcement actions beginning on July 1, 2020 (or sooner if the final regulations are published six months prior to July 1, 2020, which is also the date on which the regulations required by the CCPA are due to be final).⁴ The AGO may bring enforcement actions for non-compliance with CCPA for actions going back to the January 1, 2020 effective date, regardless of whether the final regulations were available at the time the violation occurred. The comment period for the Proposed Regulations closes December 6, 2019. It is clear that final regulations will not be ready before the January 1, 2020 effective date of CCPA, and it seems unlikely that the final regulations will be ready much before the enforcement date of July 1, 2020.

Putting aside the wisdom of the implementation schedule in CCPA,⁵ the reality is that businesses subject to CCPA began assessing compliance needs and developing the required new tools, such as the capability to opt-out of sale, months ago to work toward the January 1, 2020 effective date. Significant resources have already been put against understanding the legal requirements of the statute as they apply to a given business; hiring and training necessary staff across functional areas; and designing and coding a complex set of new capabilities. The implementation schedule in CCPA only makes sense to the extent that the AGO reads the requirements for regulations narrowly, as providing clarifications and detail consistent with the existing requirement as necessary to implement the requirements of the law.⁶ Such an approach would also be most consistent with the rulemaking mandate in the

⁴ Cal. Civ. Code § Section 1798.185(c). The August 2018 amendments (S.B. 1121) to CCPA revised the original time frame in the statute by giving the AGO more time to prepare the regulations, at the [AGO's urging](#), thus creating a framework where the CCPA law would become operative before the AGO would be required to deliver final regulations.

⁵ Though by comparison, it is notable that the EU General Data Protection Regulation ("GDPR"), which built on the requirements of its predecessor, the EU Data Protection Directive (adopted in 1995), allowed covered entities two years from publication of the final text of the Regulation to the effective date.

⁶ This approach to drafting the implementing regulations for CCPA would also be most consistent with the expectations of the California Legislature which expected that the CCPA would set the deadlines and core provisions for compliance with CCPA. The



CCPA (as originally passed and as amended by A.B. 1355) which only allows “additional regulations as necessary to further the purposes of th[e] title”⁷ and California law governing the rulemaking process.⁸

In the Proposed Regulations, the AG has taken a far broader approach than what is called for and creates new obligations beyond those contemplated in the text of the CCPA.⁹ Even assuming that the AG has the appropriate legal authority to do so,¹⁰ sound public policy dictates that the AG should not at this late date introduce new requirements that will be finalized *after* CCPA has already become operative on January 1, 2020. There is even the potential that certain CCPA regulations will not be finalized much before the date on which enforcement must begin, July 1, 2020.¹¹ Not only does this raise questions of fair warning and due process, but it also creates harms for consumers and businesses. For consumers, it makes understanding their rights and protections under CCPA a moving target and significantly harder to understand. For businesses, it adds uncertainty, increases legal costs, and punishes the responsible actors who began compliance efforts early by moving the goalposts, rendering prior work moot, and necessitating further investment. There is already a significant price tag for CCPA compliance efforts estimated at an initial cost of up to \$55 billion, according to the AGO’s Standardized Regulatory Impact Assessment (“SRIA”),¹² these regulations will be a cost-multiplier that makes the initial numbers seem reasonable by comparison.

IA Recommendation: The AGO should take a fair and reasonable approach to regulations by only adopting rules that are provided for in CCPA’s rulemaking mandate, reasonably necessary,¹³ and for which CCPA has already provided businesses with fair warning of the potential requirements in order to make the current implementation schedule for CCPA as beneficial to consumers as possible. IA provides detailed recommendations and proposed changes in *Section II: Specific Provisions* of these comments.

Senate Judiciary Bill Analysis stated, “[t]hese provisions provide clear guidance on the basics for ensuring compliance.” Senate Judiciary Committee Bill Analysis, p. 19 (June 25, 2018). Available at:

https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375 (last accessed November 19, 2019).

⁷ Cal. Civ. Code § 1798.185(b)(2)(as amended by A.B. 1355).

⁸ Rulemaking is governed by the California Administrative Procedure Act (“APA”), Government Code § 11340 *et seq.* Rulemaking must also comply with regulations adopted by the Office of Administrative Law (“OAL”), California Code of Regulations, Title 1, §§ 1-120.

⁹ See Section II, *infra*, for a further discussion of the manner in which the AGO conflicts with and/or enlarges the requirements of the CCPA in the Proposed Regulations.

¹⁰ See Section II, *infra*, for arguments that new requirements exceed the AGO’s authority.

¹¹ IA notes that CCPA, Cal. Civ. Code § 1798.185(a), requires specific regulations be issued “on or before July 1, 2020,” but that it also provides a more general rulemaking authorization that is not time bound in subsection (b). To the extent that the Proposed Regulations include provisions which exceed the rulemaking mandate in Section 1798.185(a), there does not appear to be any required due date for such regulatory provisions.

¹² Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, available at: http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

¹³ Cal. Gov. Code § 11349(a).



2. The Proposed Regulations exceed the legal authority of the AGO by altering, amending, or enlarging the CCPA, and failing to meet other requirements of California administrative procedure.

As more fully detailed below in *Section II: Specific Provisions*, the AGO exceeds its mandate to draft regulations to implement, interpret, or make specific the requirements of the CCPA by including provisions that directly contradict the language of CCPA, introduce new requirements not encompassed within the scope of CCPA and for which there is no reasonable necessity, and/or fails to meet other requirements of California's statutes and regulations for administrative procedure.¹⁴

Background on California's Rules for Promulgating Regulations

For the benefit of members of the public who may review these comments, we offer the following basic background on the APA.¹⁵ The California Government Code and its implementing regulations require that regulations adopted by agencies in the state meet procedural and substantive specifications. These specifications apply to the Proposed Regulations, the Initial Statement of Reasons ("ISOR"), and the SRIA. For example, the ISOR must explain how the Proposed Regulation is "reasonably necessary to carry out the purpose and address the problem for which it is proposed" and describe "reasonable alternatives to the regulation and the agency's reasons for rejecting those alternatives."¹⁶ The required financial analysis is intended to inform the agency and the public about whether the Proposed Regulation "is an efficient and effective means of implementing the policy decisions enacted in statute ...in the least burdensome manner."¹⁷ The Office of Administrative Law ("OAL") is tasked with reviewing Proposed Regulations, prior to enactment, for compliance with procedural requirements and substantive requirements including: (1) Necessity; (2) Authority; (3) Clarity; (4) Consistency; (5) Reference; and (6) Nonduplication.¹⁸

Where the Proposed Regulations create new requirements, such as the requirement to treat a browser signal as a valid opt-out of sale,¹⁹ the AGO fails to show sufficient authority or necessity to meet the requirements of California law. For example, with regard to browser signals the ISOR states,

¹⁴ Cal. Gov. Code § 11340 *et seq.* California Code of Regulations, Title 1, §§ 1-120. Cal. Gov. Code § 11342.2 states, "Whenever by the express or implied terms of any statute a state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute."

¹⁵ Resources for additional background are available on the website of the Office of Administrative Law, available at: oal.ca.gov. The California Architects Board website hosts a report titled "How to Participate in the Rulemaking Process" which also offers background on state requirements for promulgating regulations, available at: https://www.cab.ca.gov/docs/misc/rulemaking_process.pdf (last accessed November 25, 2019).

¹⁶ Cal. Gov. Code § 11346.2(b).

¹⁷ Cal. Gov. Code § 11346.3(e).

¹⁸ Cal. Gov. Code § 11341.1(a).

¹⁹ Proposed Regulation § 999.315.



This subdivision is intended to support innovation for privacy services that facilitate the exercise of consumer rights in furtherance of the purposes of the CCPA. This subdivision is necessary because, without it, businesses are likely to reject or ignore consumer tools.²⁰

This is ironic, because in the drafting of CPPA, reliance on existing consumer controls was rejected because of the view that having a uniform button or logo was too important to forgo. As a result the CCPA provides only one mechanism for consumer opt-out to sale - the “Do Not Sell My Personal Information” link on the business’ internet homepage.²¹ The authority provided by CCPA specifically tasked the AGO with creating rules for, “development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness.”²² Thus, it is clearly not within the rulemaking mandate from the Legislature. Nor is it consistent with the general rulemaking authorization in CCPA, allowing the AGO to “adopt additional regulations as necessary to further the purposes of this title.”²³

The record provided in the ISOR does not satisfy California law’s definition of necessity in this context. California Government Code Section 11349(a) defines “necessity” as requiring that the rulemaking record,

demonstrates by substantial evidence the need for a regulation to effectuate the purpose of the statute ... that the regulation implements, interprets, or makes specific, taking into account the totality of the record. For purposes of this standard, evidence includes, but is not limited to, facts, studies, and expert opinion.

Other than speculation in the ISOR that businesses “will likely ignore” other methods, no reasoning is offered for rejecting the approach adopted by the Legislature of having a uniform mechanism to signal to consumers how to opt-out from sale of their personal information. In addition, the ISOR provides no explanation for the adoption of browser signals and other technology as required by the APA, Cal. Gov. Code § 11346.2(b)(1), which states that,

Where the adoption or amendment of a regulation would mandate the use of specific technologies or equipment, a statement of the reasons why the agency believes these mandates or prescriptive standards are required.

Furthermore, the AGO did not include this new requirement in the discussion of reasonable alternatives in the ISOR. California Government Code Section 11346.2(b)(4) mandates consideration of reasonable alternatives. In light of readily available alternatives including following the legislative mandate of CCPA, using the “designated methods” available for access and deletion requests, or allowing companies to rely on existing opt-out programs that achieve similar goals, as well as the likelihood that such alternatives would impose substantially less burden on business, including small business, it is not clear why the AGO

²⁰ ISOR, p. 24.

²¹ Cal. Civ. Code § 1798.135(a)(1).

²² Cal. Civ. Code § 1798.185(a)(4)(C).

²³ Cal. Civ. Code § 1798.185(b)(2).



thought this was an area where reasonable alternatives did need need to be given consideration and the rejection of less burdensome alternatives justified. IA also believes that, given the technical nature of the mandates around “browser plug-ins” and other user-enabled technologies, the AGO should be required to consider performance-based alternatives under the APA.²⁴

This provision will be further discussed below in *Section II*'s analysis of Section 999.315, but it is offered here as *but one* example of how the AGO has exceeded its authority and the Proposed Regulations conflict with the requirements of California's APA.

IA Recommendation: The AGO should substantially revise the Proposed Regulations to bring them more clearly within the authority of the rulemaking powers granted by the CCPA, to ensure consistency with the clear terms of the CCPA, and to abide by the APA and its regulations. This should include another notice and comment period due to the substantial changes to the Proposed Regulations,²⁵ a new ISOR that appropriately considers reasonable alternatives,²⁶ and a new SRIA based on accurate understandings of the business impact of the regulations where they deviate from the requirements of the CCPA.²⁷

3. The Proposed Regulations place unnecessary burdens on consumers and businesses.

The Proposed Regulations impose new requirements, beyond those required by the CCPA, which will impose unnecessary burdens on consumers and businesses. These unnecessary burdens undermine the statutory intent of the CCPA, by making it more difficult for consumers to understand and exercise rights over their data created by CCPA. The unnecessary burdens to business introduce new requirements without justification, require duplicative processes, enlarge obligations contained in the CCPA, make it more difficult for businesses to comply with the requirements of the CCPA, and expand the costs of compliance far beyond what was contemplated in the SRIA prepared in connection with this rulemaking process.

Numerous examples are explained below in *Section II*'s discussion of specific provisions of the Proposed Regulations, but one notable example that harms both consumers and businesses is the Proposed Regulation's provisions on notices to consumers. Transparency regarding

²⁴ Cal. Gov. Code § 11346.2(b)(4)(A).

²⁵ Cal. Gov. Code § 11346.8(c)(restricting the ability of an agency to adopt regulations with “nonsubstantial changes” from those noticed to the public. Title 1, Section 40 of the California Code of Regulations defines “nonsubstantial changes” to mean those that “clarify without materially altering the requirements, rights, responsibilities, conditions, or prescriptions contained in the original text.” 1 C.C.R. § 40).

²⁶ Cal. Gov. Code § 11346.2(b)(4).

²⁷ Cal. Gov. Code §§ 11346.3 & 11346.36 set forth the requirements for the financial analysis for a Proposed Regulation. Due to the substantial deviations from CCPA and the baseline regulatory measures that purported to form the basis of the SRIA that was conducted, a new SRIA should be prepared that satisfies the requirement that “[t]he baseline for the regulatory analysis shall be the most cost-effective set of regulatory measures that are equally effective in achieving the purpose of the regulation in a manner that ensures full compliance with the authorizing statute or other law being implemented or made specific by the Proposed Regulation.” Cal. Gov. Code § 11346.3(e).



business practices for handling personal information is widely regarded as a core element of a strong privacy regulatory regime and is a privacy principle that IA member companies support.²⁸ California has been a leader in the U.S. in adopting transparency requirements for personal information. However, privacy regulators and privacy researchers across the globe have also noted that *more* information is not necessarily the hallmark of effective transparency, rather that effective transparency requires the communication of the most important information to inform consumer choices. The Proposed Regulations introduce numerous new required disclosures for various notices and for privacy policies that exceed the requirements of CCPA and add significantly more detail and complexity to such disclosures. While the Proposed Regulations also talk of notices needing to be in “plain language” and easily understood by consumers, any notice comprised of all the required elements in the regulations will span innumerable small screens (like those on a mobile phone) and is unlikely to attract the full attention, if any, of consumers. This conflicts with the AGO’s performance-based standards for privacy policies articulated in the regulations and with weight of concerns expressed by regulators and other privacy experts.²⁹ In fact, it arguably fails to understand that the concept of “plain language,” as used in the studies and reports the AGO cites, means more than the selection of words that are understandable to the average consumer, it means—

*A communication is in plain language if its wording, structure, and design are so clear that the intended readers can easily find what they need, understand what they find, and use that information.*³⁰

IA Recommendation: The AGO should substantially revise the requirements of the Proposed Regulations to remove unnecessary burdens on business and to ensure that consumers benefit from clear, meaningful disclosures of privacy practices and methods for exercising their data rights, such that consumer can easily find the information they need and are able to use such information, as further explained in *Section II*.

Section II. Specific Provisions of Proposed Regulations

§ 999.301 Definitions

²⁸ See IA Privacy Principles, fn. 2, *supra*.

²⁹ See, e.g., Center for Plain Language, *Privacy-policy Analysis* (2015), p. 1 (noting that a privacy policy that no one reads provides no protections), available at: <https://centerforplainlanguage.org/wp-content/uploads/2016/11/TIME-privacy-policy-analysis-report.pdf> (last accessed December 4, 2019); Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 *Fordham Intell. Prop. Media & Ent. L.J.* 181 (2016), pp. 188-89 (discussing the difficulty of being concise in privacy policies and how long it would take a consumer to read all relevant privacy notices); Schaub, et al., *A Design Space for Effective Privacy Notices*, Symposium on Usable Privacy and Security (SOUPS) 2015 at Ottawa, Canada, p. 2 (July 22-24, 2015) (explaining that requirements regulatory compliance impact the length and complexity of notices stating “privacy notices often take the shape of long privacy policies or terms of service that are necessarily complex because the respective laws, regulations, and business practices are complex” and that privacy policy typically read like contracts because regulators seek to enforce them like contracts), available at: <https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf>; See also, European Union’s Article 29 Working Party, *Guidance on Transparency*, para. 4, “The concept of transparency in the GDPR is user-centric rather than legalistic ... [T]he quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects” “succinctly in order to avoid information fatigue.”

³⁰ Center for Plain Language, *Privacy-policy Analysis*, p. 1.



- **(a) “Affirmative Authorization”** requires that consumers undergo a two-step process to indicate and then confirm their request to opt-in to sale. Elsewhere in the Proposed Regulations, a two-step process is outlined for the exercise of additional consumer rights, such as the right to delete.³¹ This two-step process introduces unnecessary friction to consumers, as well as potential risks. For example, a consumer may believe that after completing step one of the process that they have successfully performed the task and leave the process. This will result in the consumer’s intent going unfulfilled without their knowledge, and create a potential limbo state for the business which may be unsure how to treat a consumer who has initiated but not completed a process. It is important that consumers understand the significance of the action they intend to undertake, which is why CCPA requires clear consumer notices and the Proposed Regulations define “affirmative authorization” as “an action that demonstrates the intentional decision by the consumer.” This performance-based standard is preferable to a strict technical mandate to use two-steps. A business should not be able to rely on satisfying a technical requirement to have two steps, rather than satisfying an obligation to design a process that is clear to consumers and ensures they are intentionally exercising their rights. In addition, more “clicks” can be obstacles to the exercise of consumer rights and has the potential to numb consumers to the processes required to accomplish tasks associated with exercising their privacy rights.³² To avoid these results, the Proposed Regulations should establish a definition of “affirmative authorization” that is not dependent on a two-step process and then use the definition where appropriate to describe the process for a consumer to exercise a right regarding their personal information, rather than prescribing a specific two-step process in each regulatory provision addressing methods for exercise of consumer rights.

IA Recommendation: Revise the definition of “affirmative authorization” to read, “means an action that demonstrates the intentional decision by the consumer to exercise a consumer right provided by the CCPA, opt in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided consent to the sale of the child’s personal information in accordance with the methods set forth in Section 999.330. For consumers 13 years and older, it is demonstrated through two step process whereby the consumer shall first, clearly request to opt in and then second, separately confirm their choice to opt in.” Additionally, Sections 999.316(a), 999.312(d), and 999.313(d)(7) should be revised to require “affirmative authorization” rather than a “two-step process.”

- **(g) “Financial Incentive”** please see discussion of this definition and IA’s recommendations for Sections 999.307 and 999.337, *infra*.

³¹ See, § 999.312(d).

³² See, e.g., Schaub, A Design Space for Effective Privacy Notices (discussing risks of notice fatigue and habituation in response to consumer notices and choices and alternatives for increasing consumer engagement in making choices).



- **(h) “Household”** as defined, whether alone or in combination with Section 999.318, does not resolve concerns about risks to the physical safety of consumers that may result from allowing individual members of a household to obtain data that pertains to the entire household, as is discussed in detail, *infra*, in connection with Section 999.318.
- **(j), (p), and (q) “Notice of right to opt-out”; “Request to opt-out”; “Request to opt-in”** are defined in the Proposed Regulations as abbreviated terms for the longer statutory terms of “right to opt-out of sale”; “request to opt-out of sale;” and “request to opt-in to financial incentive.” While IA appreciates that adopting shorthand for these lengthy phrases is useful, we are also concerned that defaulting to these more general monikers may result in consumer confusion. First, CCPA uses the term “opt-in” in two different contexts – sales of personal information and financial incentive programs – but the definition for “request to opt-in” refers only to the sale of personal information. Presumably, a request to opt-in to a financial incentive would need to be referenced by its full description. However, consumers may be easily confused and not aware at any given time that there are different types of “opt-ins” implicated by CCPA. Likewise, requests and notices related to opt-out could apply across a range of scenarios in CCPA. In addition to the opt-out from sale referenced in the regulatory definition, “opt-out” could also apply to a withdrawal of consent following an opt-in to a financial incentive or opt-in to sale of personal information by a parent of a consumer under the age of 13. In addition, confusion over these terms may also result from the use of the terms “opt-in” and “opt-out” in other privacy laws³³ or privacy controls³⁴ that may be applicable to a consumer. Given the varying definitions and scope of the potential range of “opt-opt” and “opt-in” choices a consumer will be presented with in the course of managing the privacy of his/her personal information, the AGO should be more specific in adopting any shorthand for the rights provided by the CCPA.

IA Recommendation: Revise definitions to adopt more specific references to each type of opt-out or opt-in, such as “Sale Opt-Out/In” and “Incentive Opt-Out/In.”

- **(l) “Price or service difference”** please see discussion of this definition and IA’s recommendation for Section 999.337.
- **(s) “Typical Consumer”** is defined as “mean[ing] a natural person residing in the United States.” It is not clear from this definition how defining the term by reference to a single person leads to an understanding of what is “typical.” The Merriam-Webster Dictionary defines “typical” as “combining or exhibiting the essential characteristics of

³³ See, e.g., Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313, Subpart A (Privacy and Opt-Out Notice)(May 24, 2000); See also, HHS.gov FAQ, *Can a covered entity use existing aspects of the HIPAA Privacy Rule to give individuals the right to Opt-In or Opt-Out of electronic health information exchange?*, available at: <https://www.hhs.gov/hipaa/for-professionals/faq/555/can-a-covered-entity-use-hipaa-to-give-individuals-opt-in-or-opt-out-rights/index.html> (discussing opt-in and opt-out options under the HIPAA Statute and Rule)(last accessed November 19, 2019).

³⁴ See, e.g., the Digital Advertising Alliance’s “Your AdChoices” Opt-out), available at: <https://youradchoices.com/choices-faq> (last accessed November 19, 2019).



a group (ex: typical suburban houses).”³⁵ This definition is further confused by referencing a resident of the United States, when the CCPA defines “consumer” to mean a resident of California.³⁶ The ISOR seems to suggest that this definition is necessary for the Proposed Regulations Section 999.337(b) for purposes of determining the value of consumer data.³⁷

IA Recommendation: Incorporate a definition for “typical” drawn from standard dictionary definitions, such as “means the most usual characteristics of a natural person,”³⁸ and replace the term “average consumer” (an undefined term used within the Proposed Regulations) with the defined term “typical consumer.” Or make “average consumer” the defined term, adopting a dictionary definition such “as a level typical of a group, class, or series,”³⁹ and replace “typical consumer” throughout the Proposed Regulations. Remove reference to residency.

- **Add new subdivision (v) “Signed attestation”** should be defined to specifically allow an electronically signed attestation to be acceptable.

IA Recommendation: Add new subdivision (v) to read, “Signed attestation” means an attestation that has been signed in writing or electronically.

999.305 Notice at collection

- **Proposed regulations contradict and enlarge CCPA provisions regarding new purposes for processing personal information.** Proposed Regulation Section 999.305(a)(3) introduces a new requirement for a business to obtain “explicit consent” from a consumer before processing personal information for a new purpose beyond those disclosed in prior consumer notices. This language contradicts the clear language of CCPA which requires notice to consumers of new purposes for processing personal information in Section 1798.100(b). Notably, the CCPA does not contain any consent requirements related to collection or processing of personal information, absent the singular example where the legal guardian of a minor must “opt-in” to the sale of personal information related to the child, as provided in Section 1798.120(c).

The sole justification cited for the new explicit consent requirement states,

The purpose of these subdivisions is to implement Civil Code Section 1798.100, subdivision (b). The subdivisions make clear that a business cannot change their practices after giving the notice at collection because the consumer could have

³⁵ Available at: <https://www.merriam-webster.com/dictionary/typical> (last accessed November 19, 2019).

³⁶ Cal. Civ. Code § 1798.140(g).

³⁷ ISOR, p. 7.

³⁸ Drawn from Collins Dictionary definition of “typical,” available at: <https://www.collinsdictionary.com/us/dictionary/english/typical> (last accessed November 19, 2019).

³⁹ Merriam-Webster Dictionary, available at: <https://www.merriam-webster.com/dictionary/average> (last accessed November 21, 2019).



*reasonably relied on the information provided in the notice at collection when interacting with the business.*⁴⁰

This explanation fails to explain why the AGO applied different treatment to changes in the categories of information collected and changes for purposes of collection in the Proposed Regulations when CCPA sets the same requirement for both changes - new notice to the consumer. The Proposed Regulations require a new notice for the collection of additional categories of information, but require explicit consent for any new purposes of processing.⁴¹ The AGO has not provided an explanation of why explicit consent for new purposes of processing is required, when notice without explicit consent is sufficient for the original purposes of processing under the CCPA. Regardless of the objective, the AGO has not established that this significant new burden on business is justified, or even authorized.

IA Recommendation: This unsupported and burdensome requirement clearly exceeds the AGO's rulemaking mandate and authority and should be struck from the Proposed Regulations. Specifically, IA recommends that the second sentence of 999.305(a)(3) be revised to, "If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose.~~"

- **Confusing language in the Proposed Regulations seem to require notice *before* collection of any personal information, contradicting the clear language of the CCPA.** Section 1798.100(b) says that notice to consumers shall be provided "at or before the point of collection." Section 999.305(a)(2)(e) of the Proposed Regulations state that notice must, "be visible or accessible where a consumer will see it *before* any personal information is collected." (*emphasis added*). However, Section 999.305(a)(1) states "at or before." This could potentially be an oversight given that the Proposed Regulations and the ISOR also uses the "at or before" formulation in other areas as well.⁴² The ISOR, however, explains that,

*[t]he subdivision makes clear that businesses that collect personal information without first giving notice to the consumer are in violation of Civil Code Section 1798.100 and these corresponding regulations. It clearly prohibits the surreptitious collection of personal information.*⁴³

Given the operation of the internet, there are instances where it is impossible to provide notice before collection of personal information, particularly as that term is defined in

⁴⁰ ISOR, p. 8.

⁴¹ *Id.*

⁴² See, §§ 999.305(a)(1) & (a)(5), 999.301(i)(specifically defining "notice of collection" to be notice "at or before" time of collection); ISOR, pp. 5, 8-9, 43, 54.

⁴³ ISOR, p. 9.



the CCPA Section 1798.140(o)(1)(A) including “internet protocol address” and unique identifiers.⁴⁴ Even robust privacy regulations, such as the European Union’s General Data Protection Regulation (“GDPR”), provides:

As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided “at the time when personal data are obtained.”⁴⁵

The difficulty entities subject to the GDPR have faced trying to comply with the requirements for data collection via cookies on websites demonstrates the importance of creating clear rules that create privacy benefits for consumers. Basic internet functions require that certain technical data is transferred from a client to server in order for a user to be able to view a website and some of this data is encompassed within CCPA’s definition of personal information.⁴⁶

IA Recommendation: Amend Proposed Regulations to ensure consistent use of “at or before” language, including inserting “at or” in front of “before” in Section 999.305(a)(2)(e) of the Proposed Regulations so that it states that, “notice must be visible or accessible where a consumer will see it at or before any personal information is collected.”

- **Section 999.305 should clarify that a “notice of collection” can be satisfied by providing a link to the appropriate Section of a business’ privacy policy.** Section 999.305 requires a separate “notice of collection” in addition to the information provided in a privacy policy. The Notice can take the form of either a link to a specific section of the policy, or a discrete notice. Some legal practitioners are interpreting the Proposed Regulations to require a second notice. IA believes this is not in consumers’ best interest because it only introduces more clutter and an associated increased likelihood of confusion. The AGO should make clear that the notice of collection requirement can be satisfied via a link to the corresponding section of the privacy policy, to avoid any further confusion.

999.306 Notice of right to opt-out of sale

- **Subdivision 999.306(d)(2) adds a new requirement to treat consumers as having opted-out of sale, if their personal information is collected during a period when a**

⁴⁴ See, Lea Kessner, Building With Respect, CCPA Bugs and Engineering Commentary on the CCCPA, available at: https://buildwithrespect.com/2019/11/16/ccpa-bugs-and-engineering-commentary-on-the-california-consumer-privacy-act-regs/amp/?twitter_impression=true (last accessed November 19, 2019); See also, <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information/#when-notification-is-to-occur> (last accessed November 15, 2019).

⁴⁵ Article 29 Working Party Guidance on Transparency Principles of GDPR, para. 27, available at: https://iapp.org/media/pdf/resource_center/20180413_Article29WPTransparencyGuidelinespdf.pdf

⁴⁶ https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works



business states that it does not sell data (and/or does not provide an opt-out from sale link) is unnecessary due to existing requirements for notifying consumers of changes in business practices for personal information, and creates confusion. As discussed, *supra*, with regard to Section 999.305(a)(3), CCPA and the Proposed Regulations adequately address what notice should be provided to a consumer when a business collects new information or changes the purposes of processing information. The notice requirement under Section 999.305(a)(3) would be triggered by a change to purposes of processing such as beginning to sell personal information that has not previously been sold. This notice would, like the notice at the point of collection, allow consumers the opportunity to opt-out. This meets the stated purpose for subdivision (d) in the AGO's ISOR, to avoid "selling a consumer's personal information without giving them notice and the opportunity opt-out."⁴⁷ Thus the requirement in Section 999.306(d)(2) to treat all consumers whose information was collected while a business was not selling consumer information as having exercised the right to opt-out is unnecessary for the protection of consumers.⁴⁸

Treating consumers who provide personal information as having opt-out of sale without using a trackable opt-out measure is a confusing and difficult to implement. CCPA Section 1798.120(a) requires that a business who has received a consumer opt-out of sale to wait 12 months before asking the consumer for authorization to sell their personal data.⁴⁹ The interaction of this provision with Proposed Regulation Section 999.306(d)(2) creates confusion about when the 12-month wait period would begin. Specifically whether it would be the first date of collection or the most recent date of collection. It is also not clear whether it is consistent with the intent of the wait period in CCPA, where it ensures that a consumer who has clearly indicated a desire to opt-out from sale will not be regularly asked by a business to reconsider the opt-out. If the consumer has not been presented with a decision of whether or not opt-out previously, there is no benefit to artificially postponing the ability of a business to notify the consumer of the change in policy and the newly available opt-out mechanism.⁵⁰ If in response to notice of new purposes for personal information a consumer chooses to exercise the right to opt-out of sale, the 12 month period will begin from that date and protect the consumer from repeated requests to reverse that decision.

⁴⁷ ISOR, p. 11.

⁴⁸ IA also notes that the change in whether a business "sells" personal information could result from a change in the law, rather than a change in business practices. This is not hypothetical—the definition of "sale" proposed by the new CCPA initiative expected for the November 2020 ballot would likely require many businesses who do not sell personal information under CCPA 2018 to add an opt-out of sale mechanism. It is also unclear how an "implied" opt-out would be computed for purposes of the 12-month wait period. See "A Letter from Alistair MacTaggart," posted September 25, 2019 to Californians for Consumer Privacy's website linking to initial proposed text of ballot initiative to amend CCPA 2018, available at: <https://www.caprivacy.org/post/a-letter-from-alastair-mactaggart-board-chair-and-founder-of-californians-for-consumer-privacy> (last accessed November 25, 2019).

⁴⁹ This is implemented in Proposed Regulation Section 999.315.

⁵⁰ Clearly, once a consumer opts-out, whether in response to notice at the original point of collection or subsequent notice of a change in purposes of processing to include sale, the 12 month wait period will apply.



- **Subdivision(d)(2) also purports to apply to future activities of a business in a way that appears to restrict the ability of businesses to change their practices.** However, the CCPA does not govern a business’s future potential to sell personal information, but instead governs the practices of businesses that sell personal information at the time of processing the personal information. The proposed regulation references not only businesses that actually sell personal information but that may in the future, which exceeds the current statutory language.

IA Recommendation: Strike language in Section 999.306(d)(2) stating that consumers are to be treated as having opted out of sale if they provide personal information to a business that, at that time, states that they do not sell personal information, as follows:

- (d) A business is exempt from providing a notice of right to opt-out if:
- (1) ~~It does not, and will not, sell personal information collected during the time period during which the notice of right to opt-out is not posted, and~~
 - (2) ~~It states in its privacy policy that that it does not and will not sell personal information. A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.~~

999.307 Notice of financial incentive

- **The manner in which this Section implements the requirements of CCPA’s “non-discrimination” provision, Section 1798.125, is unclear as to its intent.** Clarity is needed as to whether Section 999.307 is intended to only apply: (1) where consumers receive a financial incentive or price or service difference in connection with the exercise of their rights of access, deletion, and opt-out of sale under CCPA; or (2) to any financial incentive or price or service difference offered by businesses in connection with simply the collection of personal information. The Proposed Regulations define a “financial incentive” by reference to these activities, stating in the ISOR that it,

means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information. Civil Code Section 1798.185, subdivision (a)(6), directs the Attorney General to establish rules and guidelines regarding financial incentive offerings, but does not define the term. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term.⁵¹

This clearly ties the term “financial incentive” to the concept of discrimination against a consumer for exercising rights provided by the CCPA. This is consistent with the CCPA,

⁵¹ ISOR, p. 5. “Financial incentive” is defined in Section 999.301(g). IA notes that the proposed definition includes the term “disclosure” which is not a defined term in CCPA or the Proposed Regulations and it is unclear to which consumer right created by the CCPA it correlates or what activities it would be intended to cover.



which bars “discriminat[ion] against a consumer because the consumer exercised any of the consumer rights under this title,”⁵² by taking actions such as “denying goods or services,” “charging different prices or rates for goods or services,” “providing a different level of quality of goods or services,” or “suggesting that the consumer will receive a different price or rate.”⁵³ The CCPA does provide for exemptions from the ban on these types of price or service differentials in Section 1798.125(a)(1) in subparagraph (a)(2) where the differential is “reasonably related to the value” of the consumer’s data. Section 1798.125(b) regulates “financial incentives” by mandating notice and consumer opt-in. The ISOR goes on to connect “financial incentives” to the exercise of consumer rights over their personal information by stating,

The definition is intended to help businesses implement the regulations by giving a name to the notice required by Civil Code Section 1798.125, subdivision (b)(2), regarding the prohibition on discrimination based on a consumer’s exercise of rights under the CCPA.⁵⁴

The ISOR also explains that a financial incentive or price or service difference is “discriminatory” if it treats consumers differently because they “exercised a right conferred by the CCPA or these regulations.”⁵⁵ For the sake of clarity, the consumer rights granted by CCPA, and for which any discrimination is barred, are understood to be the consumer right to know (encompassing both transparency regarding business practices and access to the consumer’s specific pieces of personal information), right to delete, and right to opt-out of sale.⁵⁶ If a consumer has not exercised one of these rights, then a business, by definition, could not engage in prohibited discrimination under CCPA.

However, in other areas of the Proposed Regulations and ISOR the text is less clear that financial incentives are differences in terms resulting from the exercise of consumer rights under the CCPA, or even in regard to the processing of personal information. For example, the ISOR states without any mention of discrimination or retaliation,

that “price or service difference” means any difference in the price or rate charged for any goods or services to any consumer, including through the use of discounts, financial payments, or other benefits or penalties; or any difference in

⁵² Cal. Civ. Code § 1798.125(a)(1).

⁵³ *Id.*

⁵⁴ ISOR, p. 5.; *see also* ISOR, p. 36.

⁵⁵ *Id.*, p. 36. IA notes that CCPA does not reference any new rights for consumers that may be created by regulation and that would provide a grounds for arguing a business has engaged in unlawful discrimination under Section 1798.125. The inclusion of “these regulations” in the Proposed Regulations Section 999.336(a), and in the explanatory text of the ISOR, likely exceeds the authority of the AGO.

⁵⁶ *See*, Proposed Regulation § 999.308(b) which lists these as the rights which must be disclosed in a privacy policy, in addition to the right not to be discriminated against for exercising these three rights.



*the level or quality of any goods or services offered to any consumer, including denial of goods or services to the consumer.*⁵⁷

This language is broad and in no way tied to discrimination against consumers who exercise rights under the CCPA. In subdivision(b) of Section 999.307, the Proposed Regulations add new requirements for offering financial incentives which speak to service and price differences without any connection to exercise of consumer rights under CCPA. The ISOR however makes the conclusory statement that, these new requirements are “essential to further the CCPA’s purpose of prohibiting discrimination based on a consumer’s exercise of privacy rights.” This is clearly overreaching to the extent it purports to regulate a business that offers differing levels of service or pricing based on factors *other than* the exercise of consumer rights under the CCPA. Much like a restaurant charges different prices to consumers depending on whether they order bread and water versus lobster and Champagne, there are any number of business or market factors which may justify price or quality differentials. In some cases these may relate to processing of personal information, but the fact that personal information is processed does not mean that the consumer will *by necessity* face discrimination if they exercise one of the three consumer rights provided by the CCPA.

Thus, the Proposed Regulations and any explanatory text should be clear that simply offering differing services or prices is not within the scope of regulated “financial incentives” under CCPA Section 1798.125(b), *unless* such differences are triggered by a consumer’s exercise of the rights provided under the CCPA. Non-discriminatory service and price differences fall outside of the notice and opt-in requirements that apply to financial incentive programs regulated by CCPA specifically because they potentially retaliate against consumers exercising their data rights.

IA Recommendation: The Proposed Regulations should be clarified to ensure that regulated “financial incentives” and other price or service differences are clearly connected to the exercise of consumer rights under CCPA, by revising subdivision (a)(1) to read, “The purpose of the notice of financial incentive is to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for ~~the retention or sale of a consumer’s personal information~~ refraining from exercising a right created by the CCPA so that the consumer may make an informed decision on whether to participate.”

- **Required notices of financial incentives, like other privacy disclosure requirements discussed in these comments, are overly-detailed and may be ineffective as a result of being ignored by consumers.**⁵⁸ Deleting certain Sections requiring detailed information would make it more likely that companies can succinctly describe financial

⁵⁷ *Id.*, p. 5.

⁵⁸ *See*, fn. 29, *supra*.



incentives and differences in price and service in their online privacy notices, which is permitted under §999.307 (a)(3). Detailed recommendations for information that may be duplicative and unnecessary, include:

- The portion of subdivision (b)(2) requiring businesses to point out specific categories of personal information that are implicated, as requiring such a specific disclosure could make it much more difficult for companies to direct customers to online privacy notices.
- Subdivision (b)(5) requires inclusion of data that is likely to be proprietary information of companies.

IA Recommendation:

- Revise subdivision (b)(2) as follows: A description of the material terms of the financial incentive or price of service difference, ~~including the categories of personal information that are implicated by the financial incentive or price of service difference;~~
 - Revise subdivision (b)(5) by striking “b. A description of the method the business used to calculate the value of the consumer’s data” in its entirety.⁵⁹
- **Subdivision (b)(5) creates a new obligation, not present in CCPA, to provide consumers with a specific monetary value of their data despite a lack of consensus on reliable methodology for determining such value and dubious value to consumers in using such unreliable figures as a basis for making privacy choices.** See, *infra*, IA’s comments on the requirement to provide an estimate of the value of a consumer’s data (§ 999.336) and how that value is calculated (§ 999.337).

999.308 Privacy policy

- **The Proposed Regulations expand and enlarge the required notices and privacy policies under the CCPA, creating significant challenges for consumers to parse the notices for the information needed to make informed choices.**⁶⁰ The additional requirements make meeting the “performance-based standard” set out in the Proposed Regulations more difficult for businesses. The proposed Section 999.308 expands and enlarges the requirements of the CCPA in two ways: 1) it adds new and duplicative disclosures that must be provided in “notices” and in “privacy policies”; and 2) it creates, for the first time, a requirement that “information helpful for consumers,” but not required by the CCPA, be included in privacy policies. These new requirements cause problems for consumers and businesses alike, including:

1. **The sheer volume of information required to be provided to consumers makes it nearly impossible for businesses to meet the performance-based**

⁵⁹ See also, IA comments, *infra*, of Sections 999.336-37 as pertains to Section 999.307(b)(5)(a) which IA also believes should be substantially revised, however for different reasons.

⁶⁰ See also, IA’s comments, *supra*, in Section I.3 on this topic generally.



approach in subdivision (a)(2). The performance-based approach in subdivision (a)(2) requires a privacy policy to be “easy to read and understandable to an average consumer” by complying with the following requirements:

- a. Use plain, straightforward language and avoid technical or legal jargon.
- b. Use a format that makes the policy 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.
- d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.
- e. Be available in an additional format that allows a consumer to print it out as a separate document.

Subdivision (b) requires a privacy policy contain the following information:

(1) Right to Know About Personal Information Collected, Disclosed, or Sold

- a. *Explain that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.*
- b. *Provide instructions for submitting a verifiable consumer request to know and provide links to an online request form or portal for making the request, if offered by the business.*
- c. *Describe the process the business will use to verify the consumer request, including any information the consumer must provide.*
- d. *Collection of Personal Information*

1. List the categories of consumers’ personal information the business has collected about consumers in the preceding 12 months. The notice shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

2. For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.

e. Disclosure or Sale of Personal Information

1. State whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months.



- 2. There should be a difference between a privacy policy and a privacy resource center.** Proposed Regulation Section 999.308(b)(1)(c) requires that the process for account verification, including information needed for verification, be included in the privacy policy. Including process descriptions in the privacy policy will have adverse consequences because of the importance of avoiding unnecessary changes to the privacy policy. Descriptions of processes are frequently subject to change, particularly in the light of the CCPA implementation schedule. Because the operative date of the statute is January 1, 2020 and the regulations governing the verification process will not be finalized until some time after, it is likely that most businesses will have to make changes in the processes that will be rolled out for January 1 after the regulations are final. In addition, CCPA requires that companies review and update their privacy policies at least every 12 months.⁶¹ Furthermore, CCPA and the Proposed Regulations also require that privacy policies be available in appropriate languages and available to those with disabilities. Any policy changes thus need to be translated and appropriate updates made to ensure accessibility.

Updating privacy policies is a time-consuming process that cannot happen frequently or quickly. If a company needs to change its verification practice because it has learned about security vulnerability that impacts its current practice, it will need to act quickly to change the verification process description. For this reason, this type of process-oriented information is more appropriately *linked to* from the privacy policy, but considered outside the formal policy to allow changes according to business needs, to address emerging security threats, to enhance consumer experience, or to comply with changed legal requirements. Similar arguments apply to the requirement to place metrics in the privacy policy in subdivision (b)(8).

In addition, any descriptions of information used for verification of consumer account ownership and authentication processes should not disclose details that would allow a bad actor to obtain advance notice of how they might impersonate the account holder. Failed attempts to authenticate are useful indicators of potential fraud and would justify heightened scrutiny by a business. This would also enable businesses to maintain a sufficient level of flexibility so that they can accommodate consumers who may have forgotten or changed account information. For example, consumers may no longer have access to a specific email account or phone number that they used at the time of account registration and thus may need the business to work with them to find alternate verification options.

⁶¹ Cal. Civ. Code § 1798.130(a)(5).



CCPA does not require that this information to be in the privacy policy, nor is it information that is mandated to be disclosed pursuant to CCPA's notice provisions. In fact, the most relevant language in CCPA regarding this proposed language is contained the grant of rulemaking authority to the Attorney General, Section 1798.185(a)(7) which provides authority for the AGO to establish rules to "facilitate" access "taking into account available technology, security concerns."

There is no enforcement benefit to requiring a business to detail this process information in the privacy policy as required by the Proposed Regulation since a failure to comply with consumer requests is a statutory or regulatory violation and can be enforced as such regardless of the language of a specific company privacy policy. Consumers benefit most from being able to find such information easily to facilitate the exercise of their rights under the CCPA.

IA Recommendations:

- Revise (b)(1)(b), (b)(2)(b) by striking it in its entirety or revise to reference providing only a link to instructions or webforms for submitting requests.
 - Revise (b)(1)(c), (b)(2)(c) to state: ~~Describe~~ Link to the process the business will use to verify the consumer request, ~~including any which shall include a general description of the~~ information the consumer ~~must~~ may be asked to provide.
 - Revise (b)(8) by striking it in its entirety. *See also* discussion of Section 999.317(g), *infra*.
3. **Attempts to consolidate disclosure requirements, which are spread out in the CCPA, create confusing new obligations which will inundated consumers with repetitive information not required by law.** The Proposed Regulations require extensive information to be provided in the "notices" (e.g. at collection, right to know, delete, financial incentives, etc.) and privacy policy which goes beyond the information required by CCPA and will result in redundant disclosures to consumers making notices and Privacy Policies even more difficult for consumers to parse for the information that need to make informed decisions about the privacy of their personal information. For example, subdivision (b)(1)(d)(2) requires that a privacy policy disclose *for each* category of personal information, the categories of sources, business or commercial purposes for collection, and the categories of third parties with whom information is shared. This may seem similar to the requirements of Section 1798.130(a)(5) of CCPA which specifies information to be disclosed in privacy policies, but there are notable differences. Section 1798.130(a)(5) requires: 1) a



description of consumer rights provided by the CCPA; 2) a list of categories of personal information collected in the preceding 12 months; 3) categories of personal information sold in the preceding 12 months (or a statement that personal information has not been sold); and 4) a list of categories of personal information disclosed for business purposes in the preceding 12 months. Providing each of these individual lists required by the CCPA is very different than providing listing of sources, purposes of processing, and categories of recipients for each category of personal information collected (with is to be done in a manner consistent with the categories of information in the CCPA's definition of personal information which includes 11 broad categories of information and numerous more detailed categories).⁶² For some businesses, these categories could be the same for every category of personal information and after wading through pages of disclosures consumers will have obtained little additional helpful information. For consumers who want more nuanced information, it is available from other sources such as the "Notice at Collection" which describes the purposes of processing categories of personal information or by submitting a consumer request to obtain, for example, detailed information on the categories of personal information sold and the types of entities to whom it was sold.⁶³ Essentially, the proposed regulations convert information that CCPA mandated to be available only in response to verifiable consumer requests into information disclosed generally in privacy policies.

These types of additional disclosures are inconsistent with the text of the CCPA and not justified by reasonable necessity given the availability of the information through other means that are specifically provided for by the CCPA.

IA Recommendation: Revise subdivision (b)(1)(d)(2) to conform to Cal. Civ. Code Section 1798.120(a)(5).

- **Subdivision (b)(5) does not make adequately clear that a company may still require the use of an online account to process a request, regardless of whether or not an authorized agent is used.** Please see IA comments regarding Section 999.313(c)(7), *infra*.
- **Subdivision (b) requires that a privacy policy explain "the procedure for a consumer to designate an authorized agent," a role better filled by the AGO.** This requirement would charge businesses with explaining legal processes including how to execute a power of attorney or to name an authorized representative according to the regulations promulgated by the AGO. As explained above, a business privacy policy is not the appropriate place for consumer privacy resources generally, nor for company-specific

⁶² Cal. Civ. Code § 1798.140(o).

⁶³ Cal. Civ. Code § 1798.115(a).



business processes. A business should not be put in the position of providing legal advice on the appropriate manner for designating an authorized agent. For certain types of consumer explanatory material, it may be more appropriate for the AGO to house resources for consumers that explain how best to satisfy the requirements established by the CCPA regulations.

As discussed above, IA recommends that the AGO avoid confusing the privacy policy with a privacy center. We wholeheartedly agree that consumers should be given access to helpful resources to assist in understanding privacy policies, practices, choices that may be available, and how to exercise statutorily provided rights over personal information. However, just as explained with regard to the inclusion of procedure explanations in the privacy policy, legal explanations should not be included for many of the same reasons. They are subject to change and, in the case of powers of attorney, may be governed by statute and interpretation by courts. They are also complex, and appropriate translations will take time to be prepared and vetted appropriately. Finally, in some cases, the business is not the entity that is best positioned to educate consumers on how the law applies to their specific circumstances. The risks of attempting to do so are likely to outweigh the benefits.

IA Recommendation: Strike Section 999.308(b)(5) in its entirety.

999.312 Methods for submitting requests to know and delete

- **Section 999.312 needs to be updated to reflect recent changes to the underlying statute.** Specifically, A.B. 1564 made changes to Cal. Civ. Code Section 1798.130(a)(1)(A), which now states that “[a] business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.”

IA Recommendation: Update Section 999.312 to align with recent amendments by adding a provision that mirrors the language of CCPA Section 1798.130(a)(1)(A).

- **Section 999.312 diverges from CCPA’s clear requirements regarding designated methods for submitting consumer requests.** First, the Proposed Regulations appear to potentially require a business to have three methods for requests, *e.g.* subdivision (c)(2) Example 2. CCPA simply requires a business to designate two methods. While the AGO’s rulemaking authority allows guidance, consistent with CCPA (including as amended) as to appropriate methods and the designation of additional consumer friendly options, a requirement to designate *more* methods than required by CCPA exceeds the requirements of CCPA. The ISOR fails to justify this deviation from CCPA and the additional burden on business.



The Proposed Regulations deviate from CCPA in a more burdensome and troubling way by disregarding the entire concept of “designated methods” for exercising consumer rights. Subdivision (f) requires that a business respond to all requests, *regardless of how they are submitted*, by either treating the requests as properly submitted or sending specific directions to the consumer to correct any deficiencies or follow the specified process.⁶⁴ This entirely new proposal undermines the purposes of designating methods for submitting requests and potentially expands the requirements for how a business responds to consumer requests to an untold number of potential avenues of contact.

If a business must respond to a consumer request submitted through an improper channel that will require a business to ensure that all potential avenues of contacting a business or any of its employees, representatives, contractors, service providers, etc. are monitored, all personnel are trained to recognize and determine the appropriate course of action, and are able to ensure that such response happens quickly enough to meet with 10 day deadline for confirmation of a consumer request. The language of subdivision (f) contains no limitation on the potential avenues for contact, stating “[i]f a consumer submits a request in a manner that is not one of the designated methods of submission,” the business must respond. While this opens a whole range of potential options for directly contacting the business — such as letters directed to the CEO or General Counsel; emails to random employees in roles unrelated to privacy compliance or user requests; calls to hotlines maintained for conducting employment verification, press inquiries, law enforcement emergencies, or investor relations; requests directed to agents for service of process; walk-in requests to business offices — it also raises the prospect of potentially more indirect submissions of consumer requests, including direct contact to individual employees of a business via social media or email, requests directed to outside vendors such as law firms, or even publicly posting a request directed to a business via an “at mention” on social media. Monitoring this array of channels would be incredibly burdensome for business and would be prone to systematic failures. A request directed to a single employee could sit for months without reply if the employee is on parental leave or has left the company. By contrast, a designated method for submitting a request will have a plan in place to ensure it is appropriately staffed regardless of comings and goings of individual employees. In today’s online industry, communication via “snail mail” is virtually obsolete. Because most correspondence are hard copies of documents already available electronically, marketing materials from vendors, or otherwise non-urgent materials, not all hard copy mail will be reviewed with the regularity required to respond within the Proposed Regulations required deadline.

⁶⁴ See also, ISOR, p. 16.



When this potentially endless array of channels of communication are combined with the training mandate in the Proposed Regulations, the burden becomes even more untenable. The training for personnel who are tasked with responding to consumer requests under CCPA is a reasonable requirement directly provided for in CCPA. However, if every employee of a business is converted into someone who requires training because a consumer request could be directed to them, and they must be able to recognize the nature of the request, know where to direct it or how to respond, and the appropriate timeframe for such response, it potentially amounts to every employee having to be trained on CCPA regardless of the nature of their job role or the likelihood that they will encounter a notice in the scope of their employment.

The AGO has not met its obligations to explain why this necessary, why it is consistent with CCPA's clear language regarding "designated methods," how it furthers the purposes of the CCPA in a material way, whether the burden associated has been considered and is reasonable, or even whether there are any reasonable alternatives to achieve the goal of making sure that a business does not refuse consumer requests because they are deficient based on a technicality. If this is in fact the true purpose of this Section, subdivision (f) is broader than necessary to the extent it imposes requirements on how businesses respond to requests submitted outside of designated methods.

As noted in IA's first comment to this Section referencing the need to align the Proposed Regulations to A.B. 1654, there is clear legislative intent to allow a single online submission mechanism for online companies. It would be inappropriate for this Section to deviate from the clear language of the CCPA, as amended in 2019.

IA Recommendation: Revise Section 999.312 by striking subdivision (f) in its entirety.

999.313 Requests to know and delete

- **Subdivision (a) of this Section creates new obligations and burdens on business by requiring that a business respond to a consumer request to confirm receipt and provide information on how business will respond.** While in the context of electronically submitted consumer requests, an auto-response can potentially satisfy this new requirement that is dependent on the consumer request being submitted via the "designated method" which the business has configured to send the appropriate auto-response. This is another reason why Section 999.312(f) should be struck, as is discussed above. If this requirement remains in the final regulations, businesses will face significant risks of violating the law because of a failure to provide an auto-response on channels that are not intended for processing consumer requests. Alternatively, a business would be forced to address this risk by sending a response to all inquiries of any kind a response that complies with subdivision (a). This could be very confusing to business partners, customers, job candidates, press, and other



entities that may communicate with a business about issues completely unrelated to CCPA. For channels of communication that are not electronic, the 10 day response time may also be challenging.

CCPA provides 45 days for a business to respond to consumer requests in Section 1798.130. This year, the California Legislature passed A.B. 1355 which amended this provision of the CCPA. While other changes were made to multiple provisions which include the 45 day initial response period language, the Legislature left the response deadline unchanged. In the absence of a statutory requirement for the 10 day deadline, the regulations should only add a new requirement if it is “necessary to further the purposes” of the CCPA.⁶⁵ At this point, it is unclear what benefit this requirement offers since the confirmation will only provide consumers with information that is not specific to their situation and is available in the notices and privacy policy (or as IA recommends, other privacy-related help content) mandated by the CCPA.

IA Recommendation: IA reiterates its recommendation that subdivision (f) of Section 999.312 be struck in its entirety for the additional reasons discussed in reference to Section 999.313. In addition, IA recommends that subdivision (a) of Section 999.313 be struck in its entirety.

- **Subdivision (c) is unnecessarily burdensome and duplicative, without adding additional value and transparency for consumers.** As discussed previously, the Proposed Regulations’ attempt to rearrange the CCPA’s disclosures results in redundant notices, cumbersome privacy policies, and responses to consumer requests that are likely to overwhelm consumers with information that is readily available via privacy policies and notices, potentially obscuring the personal information that is of most value in response to an access request. This subdivision requires businesses to respond to a consumer access request not only with specific pieces of personal information but also with a second set of responses—namely, customized metadata regarding the information collected for each customer, categorized in a complicated manner outlined by the statute. There are numerous reasonable alternatives to this requirement which could lower the burden of this provision: 1) a revision to Section 999.313(c) that would clarify that a company need not additionally fulfill a request to provide categories of information collected if it is also providing specific pieces of information; 2) a revision to Section 999.313(c)(10) that would not require the additional pieces of information listed there (categories of sources, business purpose, categories of parties to whom disclosed/sold and why) to be broken out for each category of information collected; 3) a revision to Section 999.313(c)(11) clarifying that use of the language specifically enumerated in either CCPA or the regulation “provides consumers a meaningful understanding of the categories listed;” 4) a revision to

⁶⁵ Cal. Civ. Code § 1798.185(b)(2)(as amended by A.B. 1355).



Section 999.313(c)(9) expanding the circumstances in which a company could rely on a generic articulation of categories in the Privacy Notice, as opposed to a customer-specific feed. For example, the regulation could be broadened to clarify that a business may refer to its privacy policy when its response would be the same for “substantially all” or “most” consumers.

IA Recommendations: Revise subdivision (c) as follows:

- (c)(2) “For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the consumer also requested specific pieces of information and the business is discloses specific pieces of information, the business is not required to respond to the request for categories of personal information. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.
- (c)(9) “In responding to a consumer’s verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer ~~as required by the CCPA. It shall not refer the consumer to the businesses’ general practices outlined in its privacy policy~~ unless its response would be the same for all most consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.”
- **Subdivision (c)(1) creates risks of inappropriate disclosure of information about a consumer in response to an unverified consumer request.** The Proposed Regulations treat verification of a consumer request as though it is appropriate to view identity verification across a spectrum of likelihood that the person making the request is the consumer, rather than as being a minimum requirement that must be satisfied. In doing so, the AGO appears to be more concerned about the potential harm to consumers that would result from not being able to access personal information, delete information, or opt-out or in than the harm that may result from bad actors inappropriately exercising a consumer right specifically to engage in illegal or malicious action. IA member companies believe that the concern should focus more clearly on the risks from bad actors. If a business is not responding appropriately to consumer requests, the CCPA provides a remedy in the form of Attorney General enforcement. But for a consumer whose personal information is inappropriately obtained, account contents deleted, or accumulated benefits of a financial incentive program stolen, there is unlikely to be an adequate remedy.



The AGO and the California Legislature know all too well how determined criminals will target consumers and their personal information. California was a leader in passing the first data breach notification requirement in the U.S. to specifically address the harms to consumers from their personal information ending up in the wrong hands. For this reason, IA believes that the Proposed Regulations should not require that a consumer request that is rejected for failing verification be converted into a request to exercise a different CCPA consumer right.

This analysis of subdivision (c)(1) is further complicated by the way the CCPA and the regulations approach categories of personal information. General disclosures of categories of personal information, such as those mandated in notices of collection or a privacy policy, pose no specific challenges since the disclosures are not consumer specific and apply broadly. However, subdivision (c)(1) contemplates disclosure of categories of personal information specific to a particular consumer in cases where there is not appropriate verification to disclose “specific pieces” of personal information. It is unclear what types of information would go beyond generally applicable disclosures of categories of personal information without themselves raising the same issues as personal information. For example, if a request was made for personal information from a company that offers security devices and security monitoring services and the request was rejected for failure to meet the verification requirements, it would not be appropriate for the business to disclose any information, even “categories,” to the individual who was unable to verify their identity. Even categories could reveal information that should remain private. For example, the business could disclose that personal information was collected for categories related to security devices, but not categories related to the monitoring service revealing that the account holder does not subscribe to this service. This information could result in a consumer being placed at risk of being targeted for a break-in.

In addition, if the business determines that categories of personal information are the same as those generally available in its privacy policy, the business is not required to send a detailed response to the consumer.

IA Recommendation: Strike language in subdivision (c)(1) mandating that a request that fails verification be considered for disclosure of categories of personal information, as follows, “For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. ~~If the request is denied in whole or in part, the business shall also evaluate the consumer’s request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subSection (e)(2).~~”



- **Subdivision (c)(3) does not fully safeguard against risks to other consumers' accounts.** Subdivision (c)(3) states, “[a] business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s account with the business, or the security of the business’s systems or networks. However, CCPA is clear that access requests shall not “adversely affect the rights and freedoms of other consumers.”⁶⁶ This limitation on the obligations under the CCPA should be reflected in this subdivision of the Proposed Regulations.

IA Recommendation: IA recommends amending this to reference security risks to personal information of other consumers as well, by revising the subdivision to read, “substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s or another consumer’s account with the business, or the security of the business’s systems or networks.”

- **Subdivisions (c)(5) & (d)(6)(a) have potential security implications and should be clarified to reduce such risks and to ensure its requirements do not encourage activity that would itself violate state or federal law.** The subdivisions require that if an access or deletion request is denied because of federal or state law, the consumer be notified of the reason why. This has potential implications for responses to from consumer seeking access to information related to law enforcement requests. If a business is prevented by law from disclosing the request, it will also be prevented by law from disclosing that a non-disclosure provision associated with a law enforcement request is the reason why the request was denied. Other reasons for denying requests could result in greater risk of fraud or security threats. In general, this subdivision should make clear that if the basis for denying a consumer request is an exception to CCPA, the business should not have to disclose the reason.

IA Recommendations:

- Revise subdivision (c)(5) as follows, “If a business denies a consumer’s verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor ~~and explain the basis for the denial~~. If the request is denied only in part, the business shall disclose the other information sought by the consumer.”
- Revise subdivision (d)(6)(a) as follows, “Inform the consumer that it will not comply with the consumer’s request ~~and describe the basis for the denial, including any statutory and regulatory exception therefor;~~”

⁶⁶ Cal. Civ. Code § 1798.145(j).



- **Subdivision (c)(7) should be clarified to specify that a business may use a password protected account to respond to consumer requests submitted via an authorized agent.** This is necessary to ensure that online accounts, particularly those for whom verified personal information such as name, address, phone numbers, and other identifying information are not needed can be used to ensure that the party who will obtain the information has been properly authenticated using the account security controls that govern the log-in process for the password protected account.

IA Recommendation: Revise subdivision (c)(7) as follows: If a business maintains a password-protected account with the consumer, it may comply with a request to know, submitted by a consumer or an authorized agent, by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

- **Subdivision (d)(1) requires that deletion requests that cannot be verified be treated as requests to opt-out, creating risks that consumers will lose potential benefits and potentially disrupt services, without ever indicating that it is their preference.** CCPA does not specify that a consumer request to opt-out of sale requires verification, however where an individual has made an attempt to verify account ownership and failed, there may be sufficient indicia that it is not the account holder. The AGO does not weigh any benefits that the consumer may associate with allowing the business to engage in the “sale” of personal information and which may form the basis of an affirmative choice not to opt-out. However, the CCPA clearly adopted an opt-out regime that is designed to put that choice in consumer hands. If the Legislature thought that the activity captured in the “opt-out of sale” provision inherently lacked any value to consumers, it could have designed CCPA differently to reflect that choice. It chose not to and the AGO should not attempt to rewrite CCPA by creating avenues where by a consumer may passively become opted-out (and unable to be invited to opt back in for a year) as though there is no value.

999.314 Service Providers

- **Subdivision (c) imposes unjustified limitations on service providers’ permissible uses of data.** These limitations contradict and go beyond the statutory definitions of “business purpose” and “service provider” in a few key ways. The CCPA explicitly exempts from “sale” disclosures to “service providers” for a broad list of enumerated “business purposes” defined under the statute, subject to certain contractual limitations.⁶⁷ Importantly, the statute defines “business purpose” to include both a business’s or a service provider’s operational purposes or other notified purposes.⁶⁸

⁶⁷ Cal. Civ. Code § 1798.140(t).

⁶⁸ Cal. Civ. Code § 1798.140(d).



The statutory text also permits a service provider to use the personal information it receives from one business for such business purposes of both that business and the service provider where the use is authorized as part of the contracted-for “services” provided to the business and is otherwise consistent with the CCPA.⁶⁹

Because business purposes may include using personal information received from one business in a way that might also provide some benefit to other businesses, the CCPA is best interpreted to permit the service provider to use the personal information that it receives in a way that might provide some benefit to itself or to its business partners, as long as such use is consistent with the business purposes identified in the written agreement between the business and the service provider and otherwise permitted by the CCPA.⁷⁰

Subdivision (c) states:

A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.

The plain text of the subdivision appears to prohibit service providers from using the personal information they receive from one entity to provide services to another person or entity, unless such services are necessary for detecting security incidents or preventing fraud or other illegal activity.

The Proposed Regulations improperly focus solely on the business purpose of the business, and ignore the fact that the statutory definition of “business purpose” also includes the use of personal information for the “service provider’s operational purposes or other notified purposes.”

Second, the activities included in the list of business purposes (such as “performing services on behalf of the business or service provider, including providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider”) may require the combination and use of personal information received from and for the benefit of multiple businesses in order to provide such services to the business that provided the data. As such, focusing solely on the business purposes of the business, as the Proposed Regulations do, would both render the language surplusage, contrary to well-established canons of statutory

⁶⁹ Cal. Civ. Code § 1798.140(v) & § 1798.140(t)(2).

⁷⁰ Cal. Civ. Code § 1798.140(v).



interpretation, as well as potentially render impermissible a number of the activities explicitly included on the list of permissible business purposes.

IA Recommendation: Revise subdivision to read, “A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, ~~or~~ protect against fraudulent or illegal activity, engage in solely internal uses, or another business purpose that is consistent with the terms of the agreement with the businesses.”

- **Subdivision (d) imposes new obligations on service providers to respond to consumer requests.** It requires that a service provider that receives but “does not comply” with a consumer’s request to know or delete must inform the consumer of the reason for the denial, explain that the consumer should submit the request directly to the business, and when feasible, provide the contact information for the business. This requirement creates new obligations for service providers not present in CCPA. In addition, it seems to recognize that in most instances the business, and not the service provider, is the correct entity to respond to a consumer request by directing a service provider to explain to the consumer that the request should be directed to the business and provide the contact information if possible. And yet, it also confusingly suggests that independent of redirecting the consumer, a denial of a consumer request must be given an explanation of why (which seems to imply that this a reason other than that the request should be directed to the business).

IA Recommendation: Subdivision (d) should be struck in its entirety.

- **The Proposed Regulations should clarify that businesses do not have to use specific contractual language as long as the language conveys the requirements of the CCPA.** This section should clarify that no specific contractual language is necessary to comply with the requirements of the CCPA regarding business arrangements between businesses and service providers. Instead language that conveys the restrictions and obligations required by CCPA suffices to not only meet statutory obligations, but also to establish the appropriate roles and responsibilities of the entities participating in the business arrangement. Due to the potential proliferation of state privacy laws, existing sector-specific federal privacy laws, and global privacy frameworks and country-specific laws, businesses should not be required to use any CCPA-specific language in contracts and business agreements to determine the nature of the business relationship and to ensure that necessary privacy and security protections apply to consumer personal information.



- **The Proposed Regulations’ clarification of who is a service provider conflicts with the CCPA and stands to subject entities outside California to CCPA without an appropriate nexus.** Subdivision (a) says that persons or entities that: (1) provide services to a person or organization that is not a “business;” and (2) that would otherwise be considered a “service provider” shall be deemed a service provider for purposes of the regulations and CCPA. The ISOR suggests that a service provider acting on behalf of an entity that is not a “business” will be subject to the “less stringent requirements” of a “service provider.”⁷¹ It specifically mentions service providers for nonprofits and government. But this change would also apply to other entities that do not qualify as a “business,” for example, because they do not “do business in California.”

The ISOR explains that this is necessary because the definition of “Service Provider” doesn’t adequately account for service providers who collect information on behalf of a business, rather than receiving information directly from the business. This appears to be a narrow problem which could be resolved with a narrow fix without expanding the requirements of the CCPA unnecessarily. By eliminating “business” from the definition of “service provider,” the AGO removes a primary nexus in CCPA to California and has a potentially sweeping impact on out-of-state commerce that is outside its regulatory purview.

999.315 Requests to opt-out

- **Subdivision (a) requires that a business provide two or more designated methods for a consumer to opt-out from sale, one of which must be an interactive webform, adding an additional requirement to the CCPA.** CCPA Sections 1798.120, 1798.130, and 1798.135 only contemplate one method for opt-out from sale which is specified in Section 1798.135(a)(1).⁷² While allowing more flexibility to businesses to adopt additional methods to offer to consumers to exercise their rights may be appropriate in terms of furthering the purposes of the title, a mandate to adopt multiple methods or to use any specific method other than the statutorily-mandated link exceeds the AGO’s rulemaking authority.

IA Recommendation: The Proposed Regulation should be revised to make the designation of any additional methods, beyond the link required in Section 1798.135(a)(1), discretionary, as follows: “A business shall provide ~~two or more~~ designated methods for submitting requests to opt-out, including, at a minimum, an

⁷¹ ISOR, p. 21.

⁷² IA notes that the proposed ballot initiative by Alastair MacTaggart, as submitted to the AGO by letter dated October 9, 2019, (as amended November 13, 2019) would add language to CCPA 2018 to incorporate the concept of “opt-out preference signals” as an alternative mechanism to the single method of a “clear and conspicuous link” required by the CCPA as currently enacted. See Section 13, amending Cal. Civ. Code § 1798.135, of the text of the ballot initiative attached to the November letter (version three). Presumably, this indicates that Mr. MacTaggart agrees that CCPA 2018 does not include this option.



interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application. A business may, at its discretion, designate additional methods by which it will accept consumer requests to opt-out of sale of personal information.”

- **There are technical and legal issues with the requirement in subdivision (c) that businesses that collect personal information from consumers online must treat consumer-enabled privacy controls as a valid request to opt-out under 1798.120.**
 - This method was not contemplated in the CCPA, as is discussed above in regard to subdivision (a). This requirement does not comply with the CA APA and regulations as it is: 1) not necessary; 2) beyond the authority of the AGO’s rulemaking mandate; 3) it has not been adequately justified in the ISOR; 4) the financial impact was not adequately considered in the SRIA; and 5) reasonable alternatives were not adequately considered.
 - The language regarding the opt-out logo or button indicates an intent for that option to be used “by all businesses to promote consumer awareness of the opportunity to opt-out...” 1798.185(a)(4)(C). The Proposed Regulations require “at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application.”
 - If the business must provide two or more designated methods and one must be the webform/button/link, the business should be able to choose the other option to designate. As is discussed in IA’s comments on Section 999.312 of the Proposed Regulations regarding designated methods to submit access and deletion requests, this provision essentially eliminates any business choice and control over how to take-in consumer requests and to ensure adequate resources, technology, and training for handling consumer requests via the designated channels. Given the serious nature of the legal obligations which are triggered by a consumer request to opt-out, businesses need to have clarity around the potential avenues by which such requests will be submitted so that they may ensure the appropriate measures are in place for compliance. Creating uncertainty about which channels could be used for making such requests sets businesses up for failure.
 - While some businesses already offer account controls which may allow opt-out from sale to occur in a manner that is secure and will allow the consumer and the business to have a shared understanding of the nature and scope of the consumer’s choice, there are significant issues of how a browser-plug in or another type of browser signal should be applied (for devices, browsers, consumers), how such a signal would interact with other rules (e.g., CCPA’s waiting period to request opt-in), and would impact other users of shared devices or shared “unique identifiers” such as IP addresses. A consumer may



think that use of a browser-based signal has an impact beyond what is technologically feasible, since it will be specific to that browser on that specific device and cannot be applied across all of the consumer’s browsers and devices without specific action from the consumer. If a consumer wants to accomplish an “account-wide” opt-out, it will need to do so through direct communication with an online business in a manner that is specifically connected to the consumer’s account. In addition, some browser or device based controls may deprive consumers of notice regarding the potential ramifications of their choice to opt-out, the availability of a financial incentive, or an alternative option that would allow the consumer a more nuanced choice than “all or nothing.”⁷³

IA Recommendation: This requirement should be made discretionary for online businesses that can implement it in a manner with adequate controls to determine the intent of the consumer to opt-out from sale and the scope of how such opt-out should be applied. This may be accomplished by revising subdivision (c) as follows, “If a business collects personal information from consumers online, the business ~~may shall~~ treat user-enabled privacy controls, such as a browser plugin or privacy 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 **if the controls allow the consumer to clearly indicate an intent to opt-out of sale, in whole or in part, for an online account maintained with the business for that browser or device, or, if known, for the consumer.**”

- **Subdivision (f) purports to make a consumer’s opt-out of sale retroactive, by requiring that a business notify each third party who purchased consumer’s personal information in the 90 days prior to the opt-out.** This is inconsistent with the CCPA and imposes a significant technical challenge and burden, neither of which are adequately considered in the ISOR or in the SRIA. Section 1798.120(d) states that, “a business that has received direction from a consumer not to sell the consumer’s personal information, ...shall be prohibited...from selling the consumer’s personal information *after* its receipt of the consumer’s direction.” (*emphasis added*) Section 1798.135(a)(4) states, “[f]or consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business.” Nothing in CCPA’s rulemaking provisions related to opt-out of sale empower the AGO to disregard the clear language of the statute and convert a forward-looking obligation into a retroactive mandate. The rulemaking provision of CCPA tasks the AG

⁷³ Version 3 of the 2020 ballot initiative to amend CCPA 2018 also acknowledges the need for rules regarding uses of opt-out signals in Section 13, by proposing an amendment to Cal. Civ. Code § 1798.135 to add as new (b)(1) a provision that allows use of opt-out preference signals that comply with technical specifications set forth in regulations to be promulgated under the statute. If the final regulations for CCPA 2018 will include a requirement to recognize an “opt-out preference signal” as currently contemplated in the Proposed Regulations, then such a rulemaking in line with the proposed rulemaking mandate in Version 3 of the 2020 ballot initiative, described with specificity in the proposed new Cal. Civ. Code § 1798.185(20), should be added.



with, “establishing rules and procedures for...business compliance with a consumer’s opt-out request.”⁷⁴

The ISOR seeks to justify the introduction of this new obligation by noting a perceived gap in the CCPA, that because the CCPA does not require businesses to disclose the specific names of third parties to whom personal information has been sold, a consumer who wants to control the sale of their information will not know all entities who have it. The ISOR states,

*Because the CCPA only requires businesses to disclose the categories of third parties with whom it sold the consumer’s information, and not their specific identities, this subdivision places the onus on the business to forward the consumer’s request to those businesses that it sold their information within the 90 days prior to receiving the consumer’s request.*⁷⁵

However, the ISOR fails to recognize the role of consumer choice in exercising the opt-out. During the 90 days prior to the consumer submitting the request to opt-out from sale, the consumer will have been on notice of the right to opt-out because they will have been provided a notice of that right through the Notice at the time of Collection,⁷⁶ the Privacy Policy,⁷⁷ and the Notice of the Right to Opt-Out of Sale (a persistent notice via a prominent link or logo).⁷⁸ The transfers that occur in those 90 days occur following notice, but before the consumer indicates a choice to opt-out to the business. The business should be able to act in reliance on the choices that consumers make to exercise their rights under CCPA. The ISOR fails to establish that consumers generally have an expectation and a desire, once they have decided to opt-out, to make that decision retroactively and that opting a consumer out of the sale of personal information on a going forward basis fails to effectuate the intent of the consumer or the intent of the California Legislature when it designed this provision.

In introducing this new requirement in the Proposed Regulations, the AGO also imposes a significant new burden on businesses. Retroactive application is not required by the rulemaking mandate in Section 1798.185(a)(4)(B), thus IA presumes the AGO relies on the more general rulemaking authority of Section 1798.185(b)(2) which allows rulemaking “as necessary to further the purposes of this title.” However, it is worth noting that the underlying premise of this change to CCPA does not merely fill in a gap in detail; it second guesses determinations of the Legislature. First, the Legislature determined that providing consumers with categories of third parties in disclosures was an appropriate balance of the burden on business and the value of transparency and consumer control over their personal information. As the ISOR makes clear, the AGO

⁷⁴ Cal. Civ. Code § 1798.185(a)(4)(B).

⁷⁵ ISOR, p. 25.

⁷⁶ Proposed regulation § 999.305(b)(3).

⁷⁷ Proposed regulation § 999.308(b)(1)(e).

⁷⁸ Proposed regulation § 999.306.



has done its own weighing of this balance and rejected it. This is beyond the AGO's authority. Second, the Legislature determined that a forwarding-looking only opt-out was the appropriate balance of these same equities. Again, the AGO has inappropriately substituted its judgment for that of the Legislature.

It is also not clear whether the AGO considered the burden on business of imposing this retroactive requirement. Other than the glancing statement that the 90 day time period is an appropriate limit to manage the burden,⁷⁹ there is no discussion of the burden, nor any consideration of reasonable alternatives in the ISOR. The SRIA does delve any deeper into the nature of this burden. Given the breadth of the definition of "sale," this burden should not be underestimated in terms of the number and complexity of different types of transactions to which it may apply. Creating an entirely new requirement to track sales and to be able to connect a specific consumer's data to specific transactions going back 90 days is a significant new burden. Developing mechanisms, whether automated or manual, to contact each party to transactions involving a specific consumer and providing them the necessary information to even identify the consumer is a daunting task as well, particularly when remaining mindful of the extraordinarily broad definition of the personal information in CCPA. For example, because of the inclusion of "unique identifiers" as personal information, if a consumer, Jane Doe, opts out from sale of personal information a business must identify all personal information associated with Jane Doe, all transactions involving sale in the past 90 days for any piece of Jane Doe's personal information including an IP address or device ID, and notify all parties to such transactions by providing sufficiently clear direction that the third party recipients can identify the information in their systems and take action to prevent further sale. Before the AGO imposes this burden, it merits consideration of less burdensome alternatives, including shorter time frames and not creating the new requirement at all.⁸⁰

IA Recommendation: Strike subdivision (f) in its entirety.

- **Subdivision (h) creates security risks for consumers and businesses by requiring a business to disclose in response to a suspected fraudulent consumer request the reason why it is believed to be fraudulent.** Subdivision (h) provides that a request to opt-out does not need to be verifiable, but a business can decline to comply if they have a "good faith, reasonable, and documented belief" that the request is fraudulent. Business must provide notice to consumer and explain why the business believes it is fraudulent. Such disclosures may harm business efforts to protect against fraud and undermine consumer protections for security and privacy. By explaining to a potential bad actor why the business has determined they are a bad actor, the business is

⁷⁹ ISOR, p. 25.

⁸⁰ By suggesting that less burdensome alternatives be considered, IA does not intend to imply, contrary to the paragraphs above, that IA believes that such alternatives are within the AGO's rulemaking authority.



essentially providing criminals with blueprints as to how to get around their fraud detection systems and protocols. Please see also IA comments, *supra*, regarding Section 999.313.

999.316 Requests to opt-in to sale after opting-out

- Please see IA comments, *supra*, regarding Section 999.301(a), the definition of “affirmative authorization” regarding the risks for requiring consumers to go through a two-step process. For the reasons explained with regard to the definition of affirmative authorization, subdivision (a) of this Section should be revised to eliminate mention of the two-step process and should be substituted with the term “affirmative authorization.”

IA Recommendation: Revise subdivision (a) to read, “Requests to opt-in to the sale of personal information shall require affirmative authorization ~~use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.~~”

999.317 Training and record-keeping

- **The training requirement in subdivision (a) is vague and overly burdensome and offers no additional protections for consumers.** The CCPA already includes reasonable training requirements for staff dedicated to handling consumer requests under the statute.⁸¹ Subdivision (a) expands this requirement to a mandate that individuals responsible for handling consumer inquiries “shall be informed of all the requirements in the CCPA and these regulations” rather than only the relevant Sections of CCPA. CCPA is a complex and difficult to understand statute that encompasses not only consumer rights but also enforcement, rulemaking authority, and security breach remedies. To require staff dedicated to handling consumer requests to be trained on *all* of CCPA, rather than the provisions which relate to consumer requests and consumer rights expands the CCPA’s training mandate in a way that is unhelpful and may lead to more confusion and less effective training. The ISOR suggests that the training mandate was expanded because of gaps in CCPA’s text. If there are specifically relevant Sections of CCPA to which the training requirement should apply because they are related to the exercise of consumer rights, then it would have been preferable for the AGO to expand the requirement to those Sections rather than the entirety of the statute and the regulations.

IA Recommendation: Strike the entirety of subdivision (a).

⁸¹ See, e.g., Cal. Civ. Code § 1798.135(a)(3) which provides, “Ensure 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 and this Section and how to direct consumer to exercise their rights under those Sections.”



- **The recordkeeping requirement in subdivision (g) is vague, imposes an unjustified burden on business without promoting transparency to consumers or accountability, and exceeds the AGO's rulemaking authority.**
 - The provisions are vague. First, the definition of “commercial purposes” in the CCPA is extremely broad.⁸² This term is seldom used in the CCPA or in the Proposed Regulations and it is unclear as to whether or not “business purposes” are encompassed or excluded from the scope. In addition, it is not clear what types of activities constitute “receipt” for commercial purposes. This is particularly troubling given the Proposed Regulations’ approach to “designated methods” for submitting requests and the inclusion of browser signals and other automated controls as “requests” to opt-out.
 - The ISOR does not support the necessity of the new tracking and reporting obligation. It simply states, “This subdivision is necessary to inform the Attorney General, policymakers, academics, and members of the public about businesses’ compliance with the CCPA.”⁸³ It further states that it considers the burden by limiting application to businesses that handle a large amount of California consumer data (10 percent of state population or more). The SRIA, however, states that “there is no detailed data on how many California consumers all companies in the state have.”⁸⁴ It “speculates” that “all firms with more than 500 employees” will be subject to the subdivision, which it states includes 9,858 businesses.
 - The SRIA “assumes,” without any cited basis, that the businesses subject to the subdivision’s recordkeeping requirements are “likely to have mature systems for identifying, processing, and analyzing personal information from their data mapping and consumer response systems, ...that there is no incremental cost of actually collecting this information.”⁸⁵ There is no reasonable basis for the SRIA to “assume” that nearly 10,000 California businesses have in place systems to determine, for example, the date of receipt of a request to opt-out of sale and the date on which the business has fully complied with the requirements of the Proposed Regulations to notify all third parties who have received the data in the 90 days prior to the consumer’s opt-out. Since businesses had no notice of the retroactive application of CCPA’s opt-out provision prior to publication of the Proposed Regulations, it would have been impossible for businesses to know of this requirement and to have already built systems capable of complying with new recordkeeping obligations in connection with it. Thus, the SRIA estimate of \$984/year per business for satisfying this obligation seems fatally flawed and inaccurate.⁸⁶

⁸² Cal. Civ. Code § 1798.140(f).

⁸³ ISOR, p. 28.

⁸⁴ SRIA, p. 26.

⁸⁵ *Id.*, p. 27.

⁸⁶ *Id.*



- Alternatives to the recordkeeping and publication requirements in the Proposed Regulations were not adequately considered. The ISOR is not clear as to what types of alternatives to detailed metrics on consumer requests were considered to achieve the goals of transparency and accountability. It appears that the only alternatives considered were not having any requirements for reporting metrics or applying the metric reporting to all businesses. While California law does not require the AGO to invent alternatives where none exist, alternatives do exist in leading privacy regimes around the globe including the GDPR. For example, the AGO could have considered an in-take mechanism for consumer complaints regarding responses to consumer requests, periodic audits of businesses, or purely internal documentation of compliance with CCPA's requirements.
- Given the lack of understanding of the nature of the burden on businesses subject to the recordkeeping requirements and the potential that the aims could be achieved through less burdensome alternatives, the subdivision should be struck from the Proposed Regulations.
- While the problems with the mismatch between the burdens of the provision and the benefits form an adequate basis for the subdivision to be deleted from the Proposed Regulations as inconsistent with the APA, it is also worth noting that CCPA does not mandate this record-keeping requirement, nor any regulations in this area. Thus, this subdivision would only be appropriate if it was determined to be "necessary" to further the purposes of CCPA. The AGO has failed to meet this threshold.
- Given that the basis for such a recordkeeping obligation would be the rulemaking authority in Cal. Civ. Code Section 1798.185(b), the AGO is not subject to a requirement to publish the regulations by July 1, 2020 and also has significant discretion to allow a period of time for businesses that would have to comply with this new obligation to build the necessary systems and come into compliance. If the AGO keeps this proposed requirement, it should allow covered businesses one year to come into compliance after the regulation take effect and after a business becomes subject to the requirement.

IA Recommendation: Subdivision (g) be struck in its entirety.

999.318 Access/Deletion for households

- **This section does not adequately address safety concerns raised with the "household" provision as it relates to access/deletion requests for several reasons:**
 - It assumes that a business will know how many individuals are members of a household which is unrealistic and an obstacle that cannot be overcome.
 - It assumes that an abusive member of a household will not coerce other members of the household to provide consent in order for the abuser to maintain control over his/her victims activities.



- It fails to establish any timeframe for the concept of household, so it is not clear whether a friend who stays in a spare room for a month while looking for a new place to live is a member of the household, is a member for just that month, or shall be considered a member of the household forever.
- It also is not clear how it will be established that a shared access point, device, IP, or other identifier is connected with a group of people who form a “household” versus, for example, a hotel business center.
- This section of the Proposed Regulations should be struck unless adequate detail can be added that explains how households should be defined, how members of a household must establish their identity as a member of the household, and how a business can determine for each household that it has received consent from each member.
- This section should also be struck unless a mechanism can be developed to ensure that members of a household cannot be coerced or intimidated into providing consent for an access or deletion request.

IA Recommendation: The AGO should strike this section in its entirety from the Proposed Regulations and further contemplate the guidance in A.B. 1355 to address the safety concerns posed by “households” in the context of access and deletion requests. Such regulations can be issued separately from the regulations required to be issued by July 1, 2020, and processing of requests related to households postponed until such time as these critical issues of physical safety can be addressed.

999.324 Verification for password-protected accounts

- **Subdivision (a) should make clear that a business may require that a consumer request submitted through an authorized agent be authenticated through a password-protected account** as discussed in IA’s comments to Section 999.313(c)(7), *supra*. In addition to IA’s prior recommendation to revise Section 999.313, IA also recommends that subdivision (a) of Section 999.324 is revised to make this explicit.

IA Recommendation: Revise subdivision (a) to read, “If a business maintains a password-protected account with the consumer, the business may require the consumer to verify the consumer’s identity through the business’s existing authentication practices for the consumer’s account, provided that the business follows the requirements in Section 999.323. A business may require the consumer to verify the consumer’s identity and the consumer’s permission to act on the request of an authorization agent through the business’s existing authentication practices for the account. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer’s data.”

999.326 Authorized agent



- **The interaction of the verification and authorized agent provisions do not provide needed clarity regarding proper verification and authentication of agents.** The verification provisions of the Proposed Regulations do not adequately explain the proper interaction of a business' discretion in authentication with the requirement that authorized agents be allowed to make requests on behalf of consumers. In addition, it is not clear how business can be expected to reasonably authenticate agents. Because of these difficulties, as IA proposed in relation to Section 999.313(d)(7) and Section 999.324, businesses should be able to rely on their authority to require consumers to use existing accounts to make requests, to also require agents must make the requests through those same accounts as a way of demonstrating the agent's authority. The verification sections of these regulations should also provide greater specificity as to how authentication of authorized agents should progress including providing more substantial guidance on the minimum evidence required and a safe harbor for businesses.
- **Regulations are not clear regarding the use of an authorized agent to exercise the various consumer rights created by CCPA.** The CCPA only specifically includes the ability to authorize another person to exercise the right to opt-out of sale.⁸⁷ As has been previously discussed in the connection with use of an authorized agent, the difficulty of authenticating the agent's identity and authorization from the consumer create significant risks for consumers and will burden businesses who will work diligently to avoid acting on fraudulent requests. Consistent with CCPA, the Proposed Regulations should restrict use of authorized agents to the exercise of the right to opt-out sale.

999.330 Minors under 13 years of age

- **The Proposed Regulations should clarify the knowledge standard.** The standard governing the "knowledge" a business must have to trigger a duty to obtain affirmative authorization for the sale of the personal information of consumers under 13 in order must be consistent with the Children's Online Privacy Protection Act ("COPPA"). Under COPPA, a website operator must obtain parental consent when it has actual knowledge that it is collecting personal information from a user who is a child, not from "children" in general. This is reflected in the COPPA statute, regulations and longstanding FTC commentary.⁸⁸ Requiring a standard different from what is required under COPPA would cause confusion and potentially complicate a business's efforts to protect

⁸⁷ Cal. Civ. Code § 1798.135(c).

⁸⁸ See, e.g., 15 U.S.C. 6502(a)(1) ("It is unlawful for . . . any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).") (emphasis added); 16 C.F.R. 312.3 ("It shall be unlawful for . . . any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part") (emphasis added); FTC, Complying with COPPA: Frequently Asked Questions A.14 ("COPPA covers operators of general audience websites or online services only where such operators have actual knowledge that a child under age 13 is the person providing personal information.").



minors and their personal information. What is more, it would be impermissible under COPPA's preemption clause.⁸⁹

- **The Proposed Regulations should be clear that a consent methodology that satisfies COPPA necessarily satisfies the “affirmative authorization” requirement of the CCPA.** Under COPPA's preemption standard, it is clear that the Attorney General may not impose additional or otherwise inconsistent consent requirements beyond those imposed by COPPA. Under COPPA and the COPPA Rule, new approved methods for parental consent may become available in the future and such methods should be available to be used by the clear terms of the CCPA regulations.
- **Subdivision (a)(1) requires “affirmative authorization” of the sale of personal information that is in “addition to any verifiable parental consent” required by COPPA creating a duplicative requirement for businesses that are covered by COPPA.** This provision could be drafted more narrowly to fit the need explained in the ISOR. The ISOR explains that “[t]his is necessary because the CCPA's prohibition on the sale of children's personal information covers information regardless of whether collected online, offline, or from a third party.”⁹⁰ IA has no objection to entities that are not subject to COPPA being required to follow CCPA requirements. However, for a business that is subject to COPPA and has a federally-complaint process to obtain consent from parents or guardians of minors, there is no justification for requiring a completely separate and secondary consent flow. This is particularly true given that the Proposed Regulations accept the adequacy of the existing COPPA parental consent mechanisms, by adopting them for the CCPA parental opt-in to sale. A more narrow provision requiring a COPPA-compliant parental consent process that also addresses opt-in to sale under the CCPA *or* a CCPA-compliant parental opt-in to sale process adequately addresses the critical interest in child safety and privacy, as well as parental interests in being empowered to make safety and privacy decisions on behalf of their young children. IA also believes that the imposition of additional requirements on “operators” regulated by COPPA is inconsistent with the preemption clause in COPPA.⁹¹

IA Recommendation: Revise subdivision (a)(1) to read, “A business that has actual knowledge that it collects or maintains the personal information of a child ~~ren~~ under the age of 13 shall utilize ~~establish, document, and comply with~~ a reasonable method, in light of available technology, for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. Verifiable parental consent that complies with the Children's Online Privacy Protection Act and regulations thereunder shall satisfy this obligation. ~~This affirmative~~

⁸⁹ See 15 U.S.C. § 6502(d) (“No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.”)

⁹⁰ ISOR, p. 34.

⁹¹ 15 U.S.C. § 6502(d).



authorization is in addition to any verifiable parental consent required under the Children’s Online Privacy Protection Act...”

999.336 Discriminatory practices

- Please also see IA comments and recommendations related to financial incentives in regards to Proposed Regulations Section 999.307, *supra*.
- **Subdivision (a) ties CCPA’s non-discrimination provisions to the exercise of consumer rights created by regulations which exceeds the AGO’s rulemaking authority.** The CCPA is clear that non-discrimination obligations only apply to the rights “created by this title.”⁹² Where the California Legislature wanted to incorporate future provisions created by AGO rulemaking in CCPA, it did so with specific language.⁹³ Thus, consistent with rules of statutory construction, an intent to include new rights created by regulation cannot be read into Section 1798.125 of CCPA. This also exceeds the rulemaking mandate in Section 1798.185(a)(6) which charges the AGO with “establishing rules and guidelines regarding financial incentive offerings.” Thus, this subdivision should be revised to be consistent with CCPA.

IA Recommendation: Revise subdivision (a) as to read, “[a] financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code Section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA ~~or these regulations.~~”

999.337 Calculating value of consumer data

- **There is no basis for a requirement to calculate and disclose the value of consumer data in CCPA.** In fact, the California Legislature had at least one bill introduced in the 2019 which would have amended CCPA to require exactly this. [A.B. 950](#) proposed to require businesses to disclose the monetary value of consumer data, but that bill did not pass. If CCPA included this requirement, such a bill would not have been necessary. In addition, unlike other bills that would have amended CCPA which were considered and ultimately passed in the same legislative session, A.B. 950 was not acted on by legislators. Where the Legislature chooses not to enact a proposal, the AGO should not legislate such proposal through the rulemaking process.
- **This new obligation is not necessary, is burdensome, and is of questionable value.** The SRIA notes a significant lack of agreement on how to value data and on whether it can be done accurately. This lack of agreement is reflected in this Section of the Proposed Regulations in that it allows a number of different methodologies for calculating the value of data. The lack of an agreed method of calculation means that the approaches taken and the resulting values will differ significantly which will limit the utility to consumers.

⁹² See Cal. Civ. Code § 1798.125(a)(1).

⁹³ See, e.g., Cal. Civ. Code § 1798.140(i) (“and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185”).



The perceived value of data is subjective, in flux and depends on context. Because data lacks clear, objective value, academics have come up with wildly different estimates for the value of certain services to people, and experts are likely to come up with differing values for other services as well. More generally, the idea of valuing personal information and it being disclosed in a general fashion will bear no relation to the actual value of the data. The actual value of personal data will be highly variable, based not just on the specific business but also larger market considerations. For example, the value of data to a business is variable, particularly as the amount of data grows.⁹⁴ Depending on other variables in a given business arrangement, the value of the personal information could also vary widely.

Concerning free, ads-based services, personalized services, people don't give up or exchange data for their experience; instead the experience is made possible by data. This is an important distinction. Data is what enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free is not that they are being compensated with people's data. It's that they make money by selling ads: these businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on objective metrics such as the number of people who see their ads or the number of people who click on their ads.

Given the significant questions about how to generate a value for data and well-founded skepticism on whether any disclosed value for data will accurately inform consumers of information related to the transaction they are considering, there is not an adequate benefit to consumers to justify the corresponding burden to business. Needless to say, undertaking an entirely new process to generate a value of data for publication to consumers will require businesses to engage in work that is not required by the CCPA, will require substantial investigation to determine the most workable methodology among those approved in the Proposed Regulation, and new legal risks for potentially publishing a figure that is challenged.

The AGO should strike this provision and allow the plain language of the CCPA to guide business and regulatory enforcement efforts on whether financial incentive programs have an appropriate correlation of value to the consumer and value to the business.

IA Recommendation: Strike Section 999.337 in its entirety.

⁹⁴ <https://www.nber.org/papers/w24334.pdf>

Message

From: Biggs, London (REI-SAC) [REDACTED]
Sent: 12/6/2019 10:36:23 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Gardner, Rick (RIS-ATL) [REDACTED]; Burton, Jon (RIS-ATL) [REDACTED]
Subject: LexisNexis Risk Solutions Comment on CCPA Regs
Attachments: LNRS Comments on CCPA Regs 12.06.19.pdf

To the Privacy Regulations Coordinator,

Thank you for the opportunity to submit written comments on behalf of LexisNexis Risk Solutions Inc. regarding the proposed regulations for implementation of the California Consumer Privacy Act. We appreciate the opportunity to share our suggestions to improve the regulations before they become final. If you have any trouble viewing the attached document or have additional questions regarding the information provided, please do not hesitate to contact me.

Sincerely,

London

London Biggs

Senior Manager, State Government Affairs – Western Region

RELX Inc.

Cell: [REDACTED]

[Elsevier](#) | [LexisNexis Legal & Professional](#) | [LexisNexis Risk Solutions](#) | [Reed Business Information](#) | [Reed Exhibitions](#)

December 6, 2019

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

**LexisNexis Risk Solutions Inc.
Comments on Proposed CCPA Regulations**

LexisNexis Risk Solutions Inc. (“LNRS”) is hereby submitting comments to the California Office of the Attorney General (“AG”) regarding the AG’s proposed regulations for the California Consumer Privacy Act of 2018 (“CCPA”). Thank you for the opportunity to submit these comments.

LNRS, a part of RELX, is a provider of information solutions that help organizations reduce risks like identity theft, fraud, and other crimes. By bringing clarity to information, LNRS helps make communities safer, insurance rates more accurate, commerce more transparent, and processes more efficient.

We are submitting these comments to highlight a significant risk to consumers posed by the proposed regulation, which states in relevant part:

§ 999.315. Requests to Opt-Out

- (h) 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.

As with much of the CCPA, this opt-out verification limitation appears to have been crafted with marketing/advertising uses in mind and not services performed on the backend of financial transactions, for example, that are intended to protect the consumer. However, due to the breadth of the definition of “sale” in the CCPA, the opt-out right also applies to “sales” of personal information in fraud prevention and identity authentication services that are designed to protect consumers from identity theft and other security risks. Data-centric services of this nature are broadly used by businesses, financial institutions, insurance companies and government agencies to prevent or investigate such activity, and such services must contain information about California residents so that individuals purporting to be California residents can be confirmed. For example:

- California residents seeking to change a credit card or business billing address may be asked to answer certain questions that only the actual resident would know (e.g., “*which of these three addresses is not one where you have previously lived?*”, etc.); or

- California residents may order merchandise online that they want delivered to an address that is not their credit card billing address. The merchant will check in the background with a service whether that address is one that is associated with the consumer (e.g., a relative's address or a second home address). If the address does not appear to be associated with the consumer, the merchant may choose to subject the purchase to a heightened security review.

With the aggressive nature and sophistication of cybercriminals, it is not hard to see the incentive for bad actors to opt-out unsuspecting consumers from fraud prevention services without their knowledge if the identity of the consumer does not have to be verified. If a consumer has been opted-out of such authentication services by a fraudster, then attempts to authenticate the consumer's identity in such ways may result in an incomplete or empty result. Organizations seeking to prevent identity theft or other crimes would then need to try improvised ways to confirm identity or choose simply to forego identity authentication. Either result would subject consumers to greater risk.

The CCPA authorizes the AG to issue regulations to "facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information." CCPA, § 1798.185(4)(A). The law neither mandates nor prohibits requiring or allowing verification procedures for such requests. Given the financial and other harm that can befall consumers when identity thieves use information online without strong fraud detection solutions in place, any regulation that restricts verification of consumer opt-out for these use cases would be inconsistent with efforts to protect consumers as well as harmful to the public interest.

The harm can be avoided by a minor revision in the proposed regulation as follows:

§ 999.315. Requests to Opt-Out

- (h) A request to opt-out need not be a verifiable consumer request. If a business, however, cannot verify the identity of a person making a request concerning personal information sold for purposes other than advertising or marketing, the business may deny the request and shall inform the requestor that their identity cannot be verified.

This change would lift the restriction on identity verification procedures that prevent harms caused by bad actors without burdening opt-out requests related to advertising or marketing.

Thank you for your consideration.



LexisNexis Risk Solutions Inc.

By: 

Rick Gardner
Corporate Counsel
LexisNexis Risk Solutions Inc.
1000 Alderman Drive
Alpharetta, GA 30005



cc: London Biggs
Senior Manager, State Government Affairs
RELX
2101 K Street
Sacramento, CA 95816



Message

From: Heather West [REDACTED]
Sent: 12/6/2019 9:50:47 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Mozilla's comments
Attachments: CCPA regulation comments.pdf

Please find attached Mozilla's comments on the proposed CCPA regulations. Thank you.

--
Heather West
Head of Policy, Americas
Mozilla
[REDACTED]



December 6th, 2019

Attn: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Via email: PrivacyRegulations@doj.ca.gov

Dear Privacy Regulations Coordinator:

Thank you for the opportunity to submit comments on your [proposed regulations](#) for the California Consumer Privacy Act of 2018 (CCPA). The CCPA will bring important privacy and data protection rights to Californians, and it is key to ensure that this implementation is well-conceived.

Mozilla is the maker of Firefox, the open-source web browser used by hundreds of millions of people. We also create new apps and tools that put people in control of their online experience, and keep the internet open and accessible to all. We're the keeper of the open web, and a trusted technology company known for the privacy and security of its products and our values-driven approach. As the makers of the Firefox browser, we recognize that we are in a unique position to enable a trusted internet. It's why we [provide our users with more control](#) within the browser and limit the data that we collect and use in accordance with our [Lean Data Practices](#). We also work to shape policy and legislation across the globe, as we have done in California.

We're here today because we believe the internet and our industry is in crisis, and real work must be done to regain the promise of the internet. Governments - from local and state to federal and international - play a huge role in realizing that promise, and in protecting the privacy of internet users. To that end, earlier this year we released a [blueprint](#) that we believe can guide comprehensive privacy legislation at any level. We are pleased to work with you and your office to realize the promise of a trusted internet that enables people to create and share.

General comments

Core to making CCPA an implementable privacy and data protection law is the clarity the related regulations need to bring. It is important that the regulations provide that clarity so that consumers are as clear as possible about their rights and companies know with reasonable certainty what is expected of them. We intend these suggestions to help define the regulations in order to provide truly meaningful controls and compliance programs that benefit consumers.

Definition of "third parties"

Any law depends on thorough and specific definitions in order to properly apply rules and responsibilities, and doubly so for a complex law like CCPA.

999.301(e) — “Categories of third parties” means types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.

For the rules around third party data collection and sale to have real impact, the definition of third parties - or that of third party collection - is key. Unfortunately, this definition seems to carve out several important stakeholders in any data-sharing economy. This definition should be clarified to note that some entities act as both a first and third party. Usually, third party interactions are defined by the context of the data collection - not whether or not the party has a direct relationship with the user. More and more, we see companies collecting data from a number of contexts: first parties, as a third party on a different site, or simply buying data directly.

For example, many social networks and online platforms collect data directly from a consumer through direct online transaction on their platform, but also from indirect methods - whether purchasing that data or by embedding tracking elements in other websites. Defining the data collection relationship by an entity as first or third party - as this definition seems to do - raises many questions around implementation and the strength of protections that CCPA will offer.

999.301(h) — “Household” means a person or group of people occupying a single dwelling.

While we recognize that your office does not have the latitude to change the application of the “household” definition in the broader law, we continue to have great concern at the use of a household as an aggregate unit for the purposes of “right to know” and “right to access”. The current household definition and implementation will be an avenue for abuse of the CCPA, and support strong regulatory guidelines on its use.

We appreciate that the verification of a household as an aggregate unit requires all members of that household. However, it is not clear whether the data received by a household with a verified request should be all data about all persons in that household, or an aggregated (and deidentified) set of information, which could somewhat protect privacy within larger households. Also, depending on the data the entity has about the household, in many circumstances even aggregated/de-identified data is still able to be identified to a person because the sample size of the household is likely to be very small. It is not clear who may be considered a member of a household; many single dwellings have transient members, or people who live there part-time. There is no way to determine whether these members are a part of the group under this definition.

Fraud and authentication

It has been broadly noted that verification of any request for information under “right to know” or “right to access” must be adequately authenticated. While these regulations significantly clarify what kind of verification is adequate, we are concerned that the authentication processes are not strong enough and may result in data being released to non-authorized persons.



For example, it will prove to be difficult to reasonably authenticate any request where a service has minimal information about a user, let alone one from a household; records may not even exist to confirm or refute any claim as to who may live in a particular household. In particular, it is unclear whether there are adequate ways to verify a consumer's request when it is submitted through a third party service. The opportunity for fraud and abuse is high particularly if the business responding to such a request does not have a meaningful opportunity to pursue their own authentication other than asking the authorized agent for proof of such authorization. There have been [multiple reports](#) from Europe about records released based on badly authenticated, or unauthenticated, requests based on the GDPR.

We strongly encourage the Attorney General's office to set a high bar on acceptable authentication for any request, and continually monitor how this provision is used, and how to improve it, on a regular basis. We hope that strong authentication methods at third parties services will facilitate a secure and trusted consumer mechanism for those who choose to use them, as well as provide a solid liability protection for companies acting on these requests in good faith.

Metrics about Personal Data Requests

999.317. Training; Record-Keeping (g)(1)

Mozilla has published a [transparency report](#) for years, and we believe in transparency as a vital tool in helping to understand requests. While our transparency report generally focuses on requests from government and law enforcement entities, we have reported the number of [Personal Data Requests](#) received under GDPR and other data protection laws since July of 2018.

We believe that everyone should have control over their personal data, understand how it's obtained and used, and be able to access, modify, or delete it. We extend these principles to all of our users regardless of when they submit a Personal Data Request, where they are located, or whether a data protection law (such as the CCPA) grants them express privacy rights.

Mozilla takes great care to avoid collecting user location as we do not need it in order to provide our service. Companies like Mozilla that extend the same personal data rights to any person and cannot determine that individual's location, will have difficulty complying with the metrics reporting as outlined in the draft regulations. We do not want to ask users who send us data access requests for additional personal information in order to comply with a metrics standard. There is no benefit to the user in providing residency information and it makes no difference when we provide the control rights universally.

In addition the specific reporting breakdowns required (for requests to know, to delete, and to opt-out) and median response times do not significantly increase the understanding of how CCPA rights are being exercised and complied with. The metrics requirements appear to assume that requests are always clear and unambiguous and are received in systems that allow for automated response time tracking.

In reality, the ways in which consumers exercise these rights are not always clear and concise; they often combine requests in vague, non-specific language and pieces of requests may be separated or handled



as a bulk action. Users may also locate, or be directed to, self-service portals where they can exercise their rights and not need to receive any company human support at all. For example, it would be difficult to ascertain whether a self-deleted account should be measured as a CCPA data request or not.

It's important to also note that companies may not use ticketing or contact systems that includes queues or other functionalities that allow them to accurately calculate median response times. But many companies, including Mozilla, rely on email for many requests where such calculations are far from simple or automated.

We respectfully suggest the metrics reporting requirements to be simplified to include only the information most salient for consumers and the Attorney General.

In conclusion

We are pleased to offer any additional explanation of these concerns to your office, or address any other topics of interest. We look forward to continuing to discuss the path forward for protecting the privacy rights of Californians, of all Americans, and indeed of everyone worldwide.

Sincerely,

Heather West
Head of Public Policy, Americas
Mozilla

Message

From: Valdivia, Arlen [REDACTED]
Sent: 12/6/2019 10:23:24 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: MPA CCPA Comment Submission
Attachments: MPA CCPA Comments Submitted 12-6-19.pdf

Attached you will find the Motion Picture Association's comments to the CCPA regulations.

Arlen Valdivia

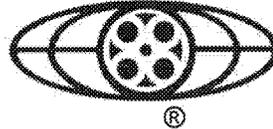
Director, State Government Affairs

E [REDACTED]

O [REDACTED] M [REDACTED]

MOTION PICTURE ASSOCIATION

15301 Ventura Blvd. | Bldg E | Sherman Oaks, CA 91403



MOTION PICTURE ASSOCIATION - AMERICA
15301 VENTURA BOULEVARD, BUILDING E
SHERMAN OAKS, CA 91403
Main: (818) 995-6600

MELISSA PATAK
VICE PRESIDENT & SR. COUNSEL
State Government Affairs

[REDACTED] - DIRECT

[REDACTED] - CELL
[REDACTED]

December 6, 2019

VIA EMAIL: PrivacyRegulations@doj.ca.gov

The Honorable Xavier Becerra
California Attorney General
Attention: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles CA 90013

Dear General Becerra:

COMMENTS OF THE MOTION PICTURE ASSOCIATION

The Motion Picture Association ("MPA") respectfully submits these comments in accordance with the California Attorney General's ("AG") proposed rulemaking, pursuant to Civil Code Section 1798.185, to implement the California Consumer Privacy Act ("CCPA").

MPA represents leading companies¹ in the creative community, including film, television, streaming content, video gaming and other content producers. We are proud to bring good jobs, high-quality entertainment and other benefits to California's economy and its consumers. Each year, we invest billions of dollars in our brands and in our trusted relationship with audiences here and globally.² We know that earning and maintaining consumers' trust is critical to our mission as businesses and good corporate citizens. Thus, we fully support efforts to ensure that consumers' personal information is handled responsibly and safely by businesses delivering desired products and services to those consumers. Regrettably, the AG's proposed regulations ("**proposed regulations**") could stifle the

¹ MPA member companies include: The Walt Disney Studios Motion Pictures; Netflix Studios, LLC; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; and Warner Bros. Entertainment Inc.

² Motion picture, television and digital entertainment production and distribution supports 2.1 million jobs, and more than \$139 billion in total wages. More than 200,000 Californians make their careers in this industry, generating over \$22 billion in wages. In addition, this sector registers a positive balance of trade in nearly every country in the world with \$16.5 billion in exports worldwide. See <https://www.motionpictures.org/what-we-do/driving-economic-growth/>

continued growth of the creative economy in California and undermine existing practices designed to protect consumer information.

We write to highlight a few implications of the proposed regulations that could impact the creative community in California.

I. The modifications to the definition of service provider exceed the scope of the CCPA and improperly limit legitimate business activity.

A. Proposed regulation

Proposed Section 999.314(c) changes the CCPA's definition of a service provider by restricting the activities a service provider can perform. First, a service provider is prohibited from using data collected from one person or entity to provide services to another person or entity. Second, the proposed regulations limit a service provider's ability to combine personal information from multiple clients only to the extent necessary to 1) detect security incidents or 2) protect against fraudulent or illegal activity.

B. Our concerns

1. The service provider restrictions exceed the scope of the CCPA.

These restrictions exceed the scope of the CCPA by impermissibly prohibiting service provider activities that would be otherwise permissible under the CCPA.

Under Section 1798.140(v) of the CCPA, a "service provider" is defined as an entity

that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

These limitations on a service provider's use of personal information are sufficiently robust to make the further restrictions in proposed Section 999.314(c) unnecessary. Nothing in the CCPA states that a service provider's use of personal information to provide services for a business precludes the use of that information for purposes that may support its services to other customers. In addition, the notion that the CCPA permits this activity only for purposes of detecting security incidents or protecting against fraud or illegal activity (but not for other purposes, such as preventing security incidents, prosecuting fraud or illegal activity, debugging or correcting errors or product improvement) is arbitrary and wholly untethered to the CCPA's statutory language.

Imposing such restrictions does not implement the statute. To the contrary, they constitute amendments to the CCPA that must be enacted through the legislative, rather than the regulatory, process.

2. The service provider restrictions would inhibit use of a wide range of business services and adversely affect the digital economy.

The regulations adopt an outdated notion of business-to-business services that assumes service providers must be “work-for-hire” contractors or providers of professional services who act exclusively for the benefit of each client. In fact, businesses increasingly leverage “software-as-a-service” and other platform-based delivery models, whereby the service provider operates a single, multi-tenant platform used by and for the benefit of multiple clients. These services are often more effective, cheaper and easier to implement and maintain precisely because all clients benefit from ongoing and iterative product improvements informed by what the service provider learns about operating the platform for all clients. What the service provider learns in the course of processing data for one client may inform a product improvement that benefits all clients. And in some cases, the services may give clients the option to get aggregated benchmarks, statistics, or other de-identified information derived from the data that the service provider processes on behalf of all clients. So long as these activities are encompassed in the definition of “services” that a business directs a vendor to perform, and the vendor is contractually prohibited from retaining, using or disclosing the business’s data for other purposes, there is no reason why the vendor cannot qualify as a service provider under the CCPA.

To arbitrarily circumscribe the scope of these activities to the detection of security incidents or prevention of fraud or illegal activity would impede the use of these services, which have been widely adopted by businesses of all types and sizes, and have been credited for fueling innovation and the growth of the digital economy over the past decade. Startups and small businesses in particular benefit from these services, which give them access to technology and capabilities they otherwise could not afford.

C. Recommendation

We recommend (i) revising proposed Section 999.314(c) to be consistent with the statutory definition of service provider; (ii) deleting the second sentence regarding data security, fraud and illegal activity; and (iii) clarifying that a business may authorize a service provider to combine personal information received from the business with personal information received from other entities to which it is a service provider, in connection with the service provider’s performance of the services specified in its contract with the authorizing business. Alternatively, we recommend deleting proposed Section 999.314(c).

II. The regulatory requirement that a business obtain explicit consent for all new uses of personal information exceeds the scope of the CCPA and imposes unnecessary restrictions on business operations and innovation.

A. Proposed regulations

Proposed Section 305(a)(3) provides that:

[i]f the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

(emphasis added).

B. Our concern

1. The explicit consent requirement exceeds the scope of the CCPA.

Section 1798.100(b) of the CCPA provides that “[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.”

Thus, a business need only give a “notice” before using the previously collected personal information for additional purposes. Upon receiving such notice, a consumer may choose to request the deletion of their personal information, to opt-out of the sale of personal information, or to receive further details about the disclosure or sale of their personal information by submitting a request under Sections 1798.100-1798.120 of the CCPA.

This conclusion is reinforced by Section 1798.140(t)(2)(D) of the CCPA, which provides that if an acquirer in a merger, acquisition or similar transaction:

materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act

Creating an additional consent requirement does not implement the statute. To the contrary, it constitutes an amendment to the CCPA that must be enacted through the legislative, rather than the regulatory, process.

2. The explicit consent requirement deviates from existing legal standards and contradicts the CCPA by failing to acknowledge the difference between material and immaterial changes.

A business may need to use data in previously undisclosed ways for a variety of administrative and other reasons that would not reasonably be expected to surprise the consumer or bear on the

consumer’s decision to entrust the business with their personal information. Recognizing this, the CCPA and most existing legal standards recognize that not every change to a privacy policy will be material to consumer expectations.

Long-standing Federal Trade Commission (FTC) guidance directs that material retroactive changes to privacy policies require opt-in consent.³ The material retroactive change standard is recognized by the CCPA itself, as we discuss in Section II.B.1 above. Under the California Online Privacy Protection Act, businesses are required to explain how they will give notice of only “material” changes to privacy policies.⁴ Finally, Europe’s General Data Protection Regulation acknowledges that consumers should reasonably expect certain data use not explicitly disclosed in privacy notices so long as it is compatible with disclosed uses.⁵

Yet, the proposed regulations deviate from the CCPA itself and other well-established legal standards by effectively requiring consent for both material and immaterial changes to notices at collection.

3. The explicit consent requirement impedes innovation, disadvantages California businesses and incentivizes creation of longer, overly-broad privacy policies.

Businesses change, products and services evolve, and the need to use data in new ways is inevitable. Yet the proposed regulation would bar these changes without the explicit consent of the business’s customers, effectively giving customers a veto right over how a company can run its business. Such an impediment would stifle innovation and the creation of new and beneficial products and services that consumers want, while placing California businesses at a competitive disadvantage.

In addition, to avoid having to seek explicit consent to new data practices, businesses may draft overly-broad privacy notices that describe all possible data uses to limit the likelihood that they will need to use data in the future in a previously undisclosed manner. This will result in longer and more confusing privacy policies that are harder for consumers to understand.

C. Recommendation

We recommend deleting proposed Section 305(a)(3) or revising it to be consistent with the CCPA requirements discussed above.

³ See, e.g., *Protecting Consumer Privacy in an Era of Rapid Change*, at vii, 15, 77 (available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>).

⁴ Cal. Bus. & Prof. Code § 22575(b)(3).

⁵ GDPR Recital 50 (“The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.”).

III. The regulatory requirement for the timing of notices exceeds the scope of the CCPA and imposes unworkable compliance obligations on businesses.

A. Proposed regulations

Proposed Section 999.305(a)(2)(e) states that the notice at collection must “[b]e visible or accessible where consumers will see it before any personal information is collected.” (emphasis added).

B. Our concerns

1. The requirement to provide notice before collection exceeds the scope of the CCPA.

Under Section 1798.100(b) of the CCPA, a business is required to give a notice at collection “at or before the point of collection.” By using only the term “before”, rather than “at or before,” the proposed regulations impermissibly narrow the CCPA’s requirement for when notice must be provided.

Imposing this additional restriction is contrary to the statute and constitutes an amendment to the CCPA that can be enacted only through the legislative process.

2. The requirement to provide notice before collection would be difficult if not impossible to comply with.

Providing notice before, rather than “at or before” the time information is being collected may be difficult or impossible, particularly in online interactions. The broad definition of personal information under the CCPA includes web-based identifiers, device-related information and electronic network activity information. These data elements are often collected automatically when visiting a website. As a result, requiring that notice be provided before any information is collected is virtually impossible, essentially requiring that notice be provided before the user reaches the website.

3. The requirement to provide notice before collection makes the proposed regulations internally inconsistent.

The proposed regulations define a notice at collection as “the notice given by a business to a consumer at or before the time a business collects personal information from the consumer as required by Civil Code Section 1798.100(b) and specified in these regulations.”⁶ This definition contradicts the requirement in proposed Section 999.305(a)(2)(e).

In addition, proposed Section 999.305(a)(2)(e) states specifically that “when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected.” Similarly, proposed Section 999.305(c) states that “[i]f a business collects personal information from a consumer online, the notice at collection may be given to the

⁶ Proposed California Consumer Privacy Act Regulations, Cal. Code Regs. Title 11, § 999.301(i) (Oct. 11, 2019) (emphasis added).

consumer by providing a link to the section of the business’s privacy policy that contains the [required] information”

Thus, while these subsequent provisions purport to allow a business to provide notice through a website privacy policy, as outlined above, this cannot be done in any practical way before any personal information is collected.

C. Recommendation

We recommend modifying Section 305(a)(2) to require notice “at or before the point of collection,” rather than before collection, thereby making this section consistent with the CCPA.

IV. The regulatory requirement that a business interpret consumer actions and signals from privacy controls as opt-out requests exceeds the scope of the CCPA, unnecessarily burdens businesses, and degrades user experience.

A. Proposed regulation

The proposed regulations include three circumstances in which a business must infer that a consumer has submitted an opt-out request, even when the consumer has not done so expressly:

1. Proposed Section 999.306(d)(2) requires that businesses that do not sell personal information, and are therefore not required to provide a notice of right to opt-out, are “deemed” to have received valid opt-out requests from all consumers whose information has been collected during a time when a notice of right to opt-out was not posted.
2. Proposed Section 999.313(d)(1) states that where a business is unable to verify the identity of a consumer submitting a request to delete data, the business must treat the unverified request as an opt-out request.
3. Proposed Sections 999.315(c) & (g) provide that businesses must interpret a consumer’s use of “privacy controls,” including those from browsers or “other mechanisms” as if the consumer has exercised an opt-out right.

B. Our concerns

- 1. The requirements to process “deemed” opt-out requests exceed the scope of the CCPA.**

Nothing in the CCPA suggests that a business must infer a consumer’s intent to submit an opt-out request without any specific direction from the consumer.

To the contrary, the consumer’s expression of choice, and a business’s responsibility to honor that choice, are at the core of the CCPA. Section 1798.130(a)(1) of the CCPA specifically establishes the method by which consumers may express the choice to opt-out, namely, a web page designated by the business. To ensure it is easy to find, the business must link to that webpage from a “Do Not Sell

My Personal Information” link placed conspicuously on its homepage. Yet the “deemed” opt-out requirements of the draft regulations disregard this statutory mechanism entirely.

Moreover, the CCPA provides that the right to opt-out applies only with respect to businesses that sell personal information (“A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information.”⁷). Further, the CCPA provides that a business must process an opt-out request only once it “has received direction from a consumer not to sell the consumer’s personal information.”⁸ A deletion request simply is not a direction to opt-out, and even if it were, the CCPA does not create a right to submit an opt-out request to a business that does not sell personal information.

Expanding a business’s opt-out obligations in this manner does not implement the statute. To the contrary, it would constitute an amendment to the CCPA that must be enacted through the legislative, rather than the regulatory, process.

2. The requirements to process “deemed” opt-out requests impose burdensome and unnecessary record-keeping and compliance requirements that undermine the principle of data minimization.

Proposed Section 999.317(b) requires that businesses maintain records related to consumer requests and how the business responded. A business that does not sell personal information, and is thus exempt under the CCPA from giving a notice of right to opt-out, would nonetheless be forced to track and maintain records of all consumer interactions involving personal information collection (potentially including all visits to the site), all of which would be “deemed” to constitute opt-out requests. This would be burdensome and costly. Furthermore, the requirement to record and report publicly on the number of consumer requests received and the company’s responses would impose an additional cost on businesses that are already devoting significant resources to building systems that enable them to respond to such requests. There is no apparent consumer benefit to making a business process and track requests to stop doing something that the business does not do.

Moreover, maintaining records about “deemed” opt-out requests undermines the principle of data minimization, a data protection principle that encourages businesses to avoid collecting more personal information than needed for the purposes for which it is collected.⁹ These requirements would require businesses to create and maintain large databases of potentially sensitive consumer data (e.g., the sites a consumer visits) without any business reason to maintain it. This practice could, in turn, harm consumer privacy if the database is compromised, all for no apparent consumer benefit.

3. Processing a “deemed” opt-out request could degrade consumer experience and expectations.

If a business is required to process an unverified deletion request or a plug-in signal as an opt-out request, the business may be required to disable personalization features that the user wants and

⁷ Cal. Civ. Code § 1798.120(a) (emphasis added).

⁸ *Id.* § 1798.120(d) (emphasis added).

⁹ *See, e.g.*, General Data Protection Regulation Art. 5(1)(c) (stating that personal data shall be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”).

expects, which could worsen consumer experience and create confusion. The proposed regulations themselves acknowledge that businesses should be able to give consumers the ability to express more granular and limited opt-out preferences so long as they have a global option to opt-out of all sales of personal information.¹⁰ By requiring businesses to treat unverified deletion requests and plug-in signals as “global” opt-out requests, the proposed regulations would inhibit a business’s ability to ensure that the request aligns with consumer expectations.

4. Requiring businesses to process “deemed” opt-out requests increases compliance costs and the risk of fraud.

Proposed Section 999.315(h) acknowledges that opt-out requests can be fraudulent, even when made explicitly. Yet the proposed regulations would require businesses to process unverified deletion requests as opt-out requests without any direction from the consumer, and even after the consumer failed to verify a deletion request, which would be an indicator of potential fraud. By providing that opt-out requests need not be verifiable, the proposed regulations assume that the only goal of fraud prevention is to protect the privacy of consumers and ignore another important goal of fraud prevention, namely, to protect businesses from the costs of dealing with fraudulent requests. This premise, combined with the obligation to treat unverified deletion requests as opt-out requests, requires businesses to bear the cost of complying with a potentially high volume of requests that consumers did not make, and that may be fraudulent.

5. Browser and plug-in based privacy controls are not a reliable mechanism for submitting opt-out requests.

A browser or plug-in signal may not give a business sufficient information to confirm the user’s intent to submit an opt-out request. Many users simply rely on default settings, meaning that the settings and information being transmitted are, in many cases, representative of the default setting rather than any particular user preference.

Moreover, a business that receives a signal from a browser setting or plug-in may not know if the user is a California resident, if the request is fraudulent, if the actual user is the person the business believes to be associated with the browser or IP address (and not someone simply sharing the device with another consumer), or what the company operating the browser or plug-in has communicated to the user about what the setting signals to websites, which is essential to understanding the user intent underlying the signal. Current browser settings and plug-ins have not been designed with the sale of personal information, as the CCPA defines those terms, in mind.

In addition, there are no recognized industry standards for these settings and there is a large and growing number of browsers and plug-ins on the global market, all of which could implement these settings in a different way. It would be extremely burdensome, if not impossible, to keep track of and comply with all possible variations of signals received from these third party products. Furthermore, protocols for browser-based default settings are still in early stages of development and requiring them to be mandatory would confuse the market and harden these protocols prematurely.

¹⁰ See Proposed California Consumer Privacy Act Regulations, Cal. Code Regs. Title 11, § 999.315(d) (Oct. 11, 2019).

C. Recommendation

We recommend removing (i) the second sentence of Section 999.306(d)(2); (ii) the second sentence of Section 999.313(d)(1); (iii) Section 999.315(c); and (iv) the third sentence of Section 999.315(g) of the proposed regulations. Alternatively, with respect to proposed Sections 999.315(c) and (g), we recommend clarifying that a business may designate which consumer-enabled privacy controls, if any, can be used to communicate an opt-out request to that business.

V. The requirements regarding valuation of consumer data exceed the scope of the CCPA and violate the right of a business to protect its trade secrets, without enhancing protection of consumer privacy.

A. Proposed regulation

Proposed Section 999.307(5) requires that businesses give consumers notice of:

- 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.

B. Our concerns

1. The requirement to disclose the valuation of consumer data exceeds the scope of the CCPA.

The CCPA requires that businesses disclose only the "material terms" of any financial incentive program and that any financial incentive be related to the value provided to the business by the consumer's data.¹¹ The CCPA simply does not require disclosure of the business's estimate of such value or the method used to calculate it. Such a disclosure requirement does not implement the statute. To the contrary, it would constitute an amendment to the CCPA that must be enacted through the legislative, rather than the regulatory, process.

2. Compliance with the requirement to disclose the valuation of consumer data would compromise confidential business information and trade secrets.

Disclosing estimates of the value of a business's assets can make it possible to infer proprietary information about the business, such as its financial performance or pricing. As such, this information is widely treated as confidential. Methods for calculating the value of a business asset commonly constitute proprietary business information and trade secrets, the development of which requires significant investment. Requiring businesses to disclose these methods would require them to compromise these trade secrets and lose the business value they confer.

¹¹ Cal. Civ. Code § 1798.125(b)(3).

In addition, disclosure of financial performance information by public companies is tightly regulated by securities laws. Information assets are no different and requiring businesses to define and disclose the purported value of the data they collect could require them to disclose proprietary information about their financial performance and/or pricing methods. Such exposures would create substantial regulatory and litigation risk, particularly for public companies.

3. The requirement to disclose the valuation of consumer data would make privacy notices longer and contribute to the problem of “notice fatigue.”

The proposed regulations require that privacy notices be “easy to read and understandable to an average consumer.”¹² Yet the CCPA’s statutory requirements alone already require businesses to substantially increase the length and complexity of privacy notices, potentially making them harder for consumers to understand and increasing the likelihood that consumers ignore them altogether. By requiring additional disclosures beyond what the text of the CCPA requires, the proposed regulations compound this problem.

C. Recommendation

We recommend that proposed Section 999.307(5) be deleted.

Thank you for your consideration.

Sincerely,

A handwritten signature in black ink that reads "Melissa Patack". The signature is written in a cursive style with a small mark at the end.

Melissa Patack

¹² Proposed California Consumer Privacy Act Regulations, Cal. Code Regs. Title 11, § 999.305(a)(2) (Oct. 11, 2019).

Message

From: Emery, Emily [REDACTED]
Sent: 12/6/2019 7:39:26 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Emery, Emily [REDACTED]
Subject: MPA Comments on the Proposed Text of Regulations Implementing CCPA
Attachments: MPA Comments on the Proposed Text of Regulations Implementing CCPA.pdf

Attached, please find comments on the proposed text of regulations implementing CCPA submitted on behalf of MPA - The Association of Magazine Media. We appreciate the opportunity to provide the attached commentary for your consideration. Please contact us if we can be of assistance.

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

December 6, 2019

The Honorable Xavier Becerra
California Department of Justice
ATTN: 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 Proposed Text of Regulations Implementing the California Consumer Privacy Act (CCPA)

Dear Attorney General Becerra:

MPA – the Association of Magazine Media (MPA) appreciates the opportunity to submit comments on behalf of its members to the California Office of the Attorney General (“OAG”) in response to the proposed rulemaking implementing the California Consumer Privacy Act (“CCPA”).

MPA represents more than 500 magazine media brands that span a vast range of genres across print, digital, mobile and video media. MPA members inform, inspire and entertain more than 90 percent of all U.S. adults through the print and digital magazine titles they trust and value most.¹ MPA members publish some of the nation’s best known, well-trusted, and most loved magazines.

Readers trust magazine media. In fact, as of 2019, traditional media sources such as magazines outpaced online-only media, owned media, and social media in terms of consumer trust.² Consistent with maintaining reader trust, MPA supports the overarching consumer protection goals of the CCPA. MPA believes that consumers should have meaningful data privacy protections, meaningful control over the use of their personal information, and greater transparency into businesses’ data practices.

Magazine media brands depend on consumer data to deliver to readers the insightful, meaningful, and world-changing content they expect. The responsible use of consumer data enables magazine media brands to understand their readers’ interests and preferences in order to personalize the content that is relevant to their readership. Data also plays a vital role for magazine publishers in helping them reach new, diverse audiences that would otherwise be

¹ MPA, *Magazine Media Factbook* (2019), available at https://www.magazine.org/Magazine/Research_and_Resources_Pages/MPA_Factbook

² Ibid.

unaware of or not have access to their content. Data allows magazine publishers to broaden their reach and create new offerings so the industry can remain relevant to consumers and do so in a way that makes magazine media accessible to readers.

In addition to data-driven content creation, magazine publishers rely on data-driven advertising to subsidize their content and to connect their readers with products and services that appeal to them. While revenue models vary by publisher, advertising is a significant source of magazine revenue for many magazine brands, and advertising revenue is crucial to magazine media's bottom line and the ability for magazine publishers to continue engaging readers. MPA members work with advertisers and agencies to deliver the right message to readers at the right time across a multitude of channels such as print, digital, mobile, and video.

In the digital space, this data-driven form of advertising is often done in a privacy-protective manner by not identifying specific consumers by name, email or other personally identifiable information. Instead, non-identifiable or pseudonymized information is used to connect relevant advertisements to browsers and devices, and such information is kept separate from consumer identities. Further, the increased adoption of contextual advertising speaks to the important first-party relationship between magazine publishers and their readers, who trust magazine publishers to serve both content and advertising that is relevant to their interests.

Magazine publishers recognize that consumers benefit from strong and effective data privacy protections, and consumer privacy protections can be effective without inhibiting consumers' ability to connect with magazines and access content they value. The success of such protections relies on the ability of businesses to correctly interpret and implement reasonable regulations into their processes for managing consumer data.

In contrast, disruptions or uncertainty around implementation could curtail the availability of the data that supports the magazine media industry. As a result, consumers could be severely impacted by diminished service offerings that cut off access to the most relevant news and content that fuels readers' interests and engagement in the world at large. In that spirit, MPA seeks additional clarifications from the OAG on the regulations, which would further enable magazine publishers to preserve the trusted relationship between readers and their magazine brands.

Uncertainty about CCPA rulemaking language poses considerable challenges for MPA members and magazine publishing as a whole. Without further clarity on the regulations and enforcement by the OAG, the implementation of the CCPA could inadvertently diminish the diverse, informative, and expert voices of magazine media, and consumers may face restricted access to the valuable content they enjoy and want.

Given the critical importance of protecting consumer data and given the short timeframe before the January 1, 2020 effective date of the CCPA, MPA commends the OAG's focus on receiving feedback on the provisions of the proposed CCPA regulations that could potentially raise implementation challenges or inadvertently undermine benefits to consumer privacy and to consumer well-being.

The CCPA could have a significant impact on the consumers of magazine media, the availability of magazine content, and the viability of magazine brands. Therefore, MPA urges the OAG to issue expedited clarifications on businesses' obligations in honoring opt-out of sale requests where consumer intent is unclear; further guidance on processing deletion requests; confirmation that varied subscription rates and metered paywalls are reasonable practices and should be exempted from financial incentive requirements; and clarifications concerning several outstanding technical implementation issues inherent in the CCPA.

I. The OAG should issue further clarification on obligations for businesses in honoring consumers' opt-out of sale requests pursuant to section 999.315.

In order to ensure that consumers have a full understanding of their rights, the business entities that handle consumer data must have clarity on their obligations under the CCPA. As mentioned above, as businesses, magazine publishers have a trusted, direct relationship with readers. Accordingly, magazine publishers take great efforts to understand and implement the serving of content and advertising based on consumer choice and engage in behaviors that support the reasonable expectation of consumers in how their data will be utilized.

MPA notes two issues with section 999.315 of the proposed OAG regulations on requests to opt-out of the sale of personal information that could circumvent consumer choice and frustrate a consumer's desired interaction with a magazine publisher's content.

In section 999.315(c), MPA believes that the OAG's direction to businesses to treat a "browser plugin or privacy setting or other mechanism... as a valid request" to opt out of personal information sale could be interpreted as a requirement to accept default browser settings that remove the ability of the consumer to choose an optimized experience on a specific website or mobile application. Particularly for businesses with a direct first-party relationship with the consumer, such as magazine publishers and their readers, the utilization of a prominently displayed "Do Not Sell My Info" link is a mechanism that is much better suited and more likely to capture a consumer's individualized preferences than a default browser setting.

This diminished consumer choice is compounded by the requirement for businesses to pass of opt-out of sale requests to all third parties that have received personal information about the consumer from the business in the past 90 days in section 999.315(f). A default browser setting could override a consumer's individual ability to engage with a business that they did not intend to restrict, even before the consumer engages with the business, resulting in a potentially negative consumer experience that removes consumer choice and overlooks individualized consumer preferences and choices.

Such a clarification from the OAG would help consumers fully actualize their CCPA rights, maintain their ability to make granular choices about data, and help ensure continued access to the magazine media content consumers wish to receive. It would also provide more certainty in the marketplace and help magazine publishers and the companies they work with understand their obligations in complying with the CCPA. Absent a clarification on the above, MPA fears these questions will diminish consumer choice, and continue to cause uncertainty for consumers and businesses alike.

II. The OAG should issue further guidance for businesses on processing deletion requests in section 999.313(d).

In the interest of respecting consumer preference regarding a request for deletion, MPA urges the OAG to clarify that businesses can retain suppression records in order to honor a consumer's deletion request. A strict application of the requirement articulated in section 999.313(d)(2) could potentially result in a business inadvertently re-adding a consumer who made a request for deletion to the business's systems if the business receives the data about the consumer from a third party after the consumer's direct deletion request was honored and processed by the business.

MPA urges the OAG to clarify in section 999.313(d)(5) that a business may "*maintain a record of the request, **including a suppression record***" in order to honor a consumer's request for deletion and to meet consumer intent in instances where the business receives information about a consumer after the initial processing of the consumer's request to delete.

III. The OAG should consider reasonable business practices where the collection of personal information for the offer of financial incentives may not be directly tied to "the value of the consumer's data" and should reevaluate the requirement to provide certain information in a notice of financial incentive in section 999.307.

The enduring relationship between reader and magazine brand is both fundamental to the industry's relevance and its business model. Accordingly, transparent, customer-forward practices are one of the industry's highest priorities. One mechanism to incentivize and preserve a long-term relationship between consumers and magazine brands is to offer discounted subscription offers to engage or retain readers. Similarly, some magazine publishers maintain paywalls in order to help readers explore available content and incentivize subscription or membership. In order to make such offers available to a reader and encourage engagement, a publisher may retain personal information about a consumer in order to track the offer and honor its redemption when the consumer elects to subscribe.

In section 999.336(a), the proposed regulations state that a price or service difference offered to consumers is prohibited if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or the proposed regulations. However, per section 999.336(b), businesses may offer price or service differences to consumers if those differences are "reasonably related to the value of the consumer's data" to the business. This requirement forces businesses to provide numerical justifications for offering benefits to consumers in the form of lower prices. The value of such incentives are often derived not from the value of a consumer's data, but instead are reasonably related to the value of the provided subscription itself. The proposed regulations' requirement, unfortunately, does not fully account for the ways in which magazine brands typically price and value their subscription offers and paywalled content. Therefore, it is not clear how the proposed regulation applies in the context of subscriptions and paywalled content.

Moreover, under section 999.307(a)(1) as currently drafted, the act of collecting and retaining personal information about a consumer coupled with standard magazine media subscription

practices could inadvertently trigger a requirement to display a “notice of financial incentive,” that must contain a “good-faith estimate of the value of the consumer’s data” and a “description of the method the business used to calculate the value of the consumer’s data.” This requirement could prompt conflicting “economic” analyses of the value of the consumer’s data based on the approved methods for making such valuations as set forth in section 999.307(b)(5)) or prompt contradictory, subjective determinations of value based on other business factor.

As a result, this requirement stands to confuse consumers rather than provide them with useful, educational information about business practices, and prove onerous for businesses to implement. Additionally, it could obligate businesses to reveal confidential or proprietary information about their valuation metrics.

MPA urges the OAG to consider whether additional clarifying language is necessary given that subscription offers and paywall models represent common business practices that collect user data in order to offer benefits to consumers. MPA recommends that the OAG consider removing the requirement to justify a price or service difference offered to consumers by ensuring such price or service difference is “reasonably related to the value of the consumer’s data,” and that the OAG consider removing the requirement to provide an estimate of the “value of the consumer’s data” and the method used to calculate such value in a notice of financial incentive.

IV. The OAG should provide further guidance on the following technical implementation issues: how businesses can provide required notices in an “alternative form” to disabled consumers; methods for providing notice at collection; design implementation for the opt-out button or logo; and the threshold for additional reporting requirements.

MPA encourages further clarification from the OAG on the following four technical implementation issues that have been raised by magazine publishers in response to their efforts to successfully implement the CCPA:

- (A) Disability access in sections 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2)(d), and 999.308(a)(2)(d).** MPA acknowledges the importance of providing access to required notices to all users, including those with disabilities. However, despite good-faith efforts, differing interpretations on whether a given “alternative form” is sufficient as indicated in sections 999.305(a)(2)(d); 999.306(a)(2)(d); 999.307(a)(2)(d); and 999.308(a)(2)(d) could result in liability exposure or litigation.

MPA recommends the OAG cite specific “alternative form” standards that have been established under existing California laws or the Americans with Disabilities Act Accessibility Guidelines as permissible methods of communicating required notices to consumers with disabilities. Further clarification from the OAG on which alternative forms are acceptable would better promote consumer access to required notices and provide helpful guidance for businesses.

- (B) Notice at collection in section 999.305.** MPA encourages the OAG to make two clarifications to facilitate the implementation of the notice at collection requirements in section 999.305. First, website displays are not static and technological innovation

continues to reshape user interfaces. Therefore, MPA encourages the OAG to affirm that providing a link to a privacy policy that contains the necessary disclosure is sufficient for notice at collection on websites or mobile application pages that feature visual displays like infinite scroll, and to indicate that the leading proposed compliance software modules are sufficient. Second, the OAG should confirm that to provide notice at the point of collection of personal information, it is sufficient for a business to provide a link to a privacy policy that contains a description of the purposes for which the data is used in “the notice on printed forms.”

MPA recommends that the OAG modify the regulatory text in section 999.305(b)(4) as follows: “*A link to the business’s privacy policy, or in the case of offline or printed form notices, the web address of the business’s privacy policy.*” This clarification would mirror language in section 999.306(c)(4), and aid in compliance where consumer information is collected from a printed paper form that is then mailed by the consumer.

(C) Outstanding button or logo instructions in section 999.306(e). MPA urgently notes that significant technical resources are required in order for businesses to implement display and functionality changes to websites and mobile applications. MPA recommends that the OAG issue its requirements and design specifications for the “Opt-Out Button or Logo” in section 999.306(e), as well as provide a public comment period for interested parties to submit input on such requirements, as soon as it is feasible. MPA also asks the OAG to explicitly indicate that leading proposed industry solutions are sufficient.

(D) Reporting threshold in section 999.317(g). MPA urges the OAG to aid smaller and mid-market businesses from overly burdensome compliance requirements by raising the reporting threshold indicated in section 999.317(g) for businesses that buy, receive, sell or share the personal information from consumers. MPA recommends that the OAG revise the threshold from 4,000,000 consumers to 10,000,000 consumers, as this number would provide relief for start-up, small and mid-market businesses. MPA further urges the OAG to clarify whether the reporting requirement is calculated on an annual or lifetime basis, and MPA recommends the requirement be calculated on an annual basis.

The CCPA sets forth a number of new requirements that stand to significantly impact the magazine publishing industry. As a result, flexibility in implementation mechanisms is crucial to enable magazine publishers to identify privacy-protective ways to comply with the law without threatening the viability of the magazine media brands that consumers enjoy. The OAG’s directives on the above technical issues will significantly improve consistent application of the CCPA across businesses and enhance the consumer experience online.

* * *

MPA – the Association of Magazine Media commends the OAG’s thoughtful approach to promulgating rules to implement the CCPA and soliciting diverse viewpoints on outstanding CCPA implementation concerns.

We are confident that further guidance by the OAG will enhance consumer privacy by placing meaningful guardrails around businesses' sale of data while simultaneously allowing longstanding industries, like the magazine media industry, to remain viable and continue to provide the data-driven content and offerings that consumers value and expect.

MPA and our members appreciate the opportunity to provide our views for your consideration, and we look forward to working with you and your staff to address the concerns outlined above.

Sincerely,

Brigitte Schmidt Gwyn
Executive Vice President

Emily Emery
Director of Digital Policy

Message

From: Mahlet Makonnen [REDACTED]
Sent: 12/5/2019 9:47:10 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: NAFCU's Comment Letter RE CCPA Proposed Regulations
Attachments: NAFCU Letter to CA AG_CCPA_12.05.19.pdf

Good Afternoon,

Please see attached for NAFCU's comment letter regarding the CCPA Proposed Regulations.

Thank you for the opportunity to submit comments on this important matter.

Best,
Mahlet

Mahlet Makonnen

Regulatory Affairs Counsel
National Association of Federally-Insured Credit Unions (NAFCU)
3138 10th Street North
Arlington, VA 22201
Office: [REDACTED]
Cell: [REDACTED]

www.nafcu.org

NAFCU | Your Direct Connection to Federal Advocacy, Education, & Compliance.



Information provided in this email represents the opinions of the author and is intended for informational purposes only. It does not constitute legal advice. If such advice or a legal opinion is required, please consult with competent local counsel.



3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

December 5, 2019

The Honorable Xavier Becerra
Attorney General
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

RE: Proposed Regulations for the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response California Department of Justice's request for comments regarding proposed regulations under the California Consumer Privacy Act of 2018 (CCPA) (Proposed Regulations). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 118 million consumers with personal and small business financial service products. NAFCU's member credit unions support a uniform federal standard, not a patchwork of state privacy laws, to protect their member-owners' data. NAFCU opposes the application of the CCPA to credit unions as they are already subject to the requirements of the *Gramm-Leach-Bliley Act* (GLBA) and are responsible stewards of sensitive consumer data.

State data privacy requirements, including the CCPA, are already creating confusion and leading to daunting compliance considerations for credit unions. In particular, the proposed CCPA regulations create challenging and expensive new obligations and varying standards that will undoubtedly present unnecessary burdens for credit unions and could, in turn, increase costs for consumers. Credit unions already comply with privacy requirements under the GLBA, yet the Proposed Regulations add overlapping and confusing requirements that would result in substantial additional compliance costs. NAFCU supports a comprehensive federal data privacy standard that builds on existing requirements under the GLBA, preempts state privacy laws, and protects consumers' information instead of a patchwork of state laws that could establish conflicting requirements, cause confusion, and significantly increase compliance costs for credit unions.

General Comments

The mounting uncertainty and rising compliance burdens related to data privacy protection from state regulators imposes undue burden on credit unions, especially those credit unions that operate across multiple states. Credit unions should not be subject to potentially 50 conflicting state privacy requirements. NAFCU advocates for a uniform federal privacy standard that would better

protect consumers and preempts state laws, including the CCPA, that pose a significant cost and strategic risk to credit unions.

A patchwork of state privacy standards will undoubtedly result in undue burden for credit unions who already comply with federal privacy requirements, such as the GLBA. The impact of privacy laws in varying jurisdictions would also lead to a chilling effect on the products and services credit unions are able to offer to consumers. Accordingly, NAFCU supports a federal privacy law that protects consumers, holds all entities accountable, and recognizes existing federal privacy laws financial institutions follow. NAFCU advocates for the following six principles to be included in a federal privacy law:

1. A comprehensive national data security standard covering all entities that collect and store consumer information.
2. Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.
3. Delegation of enforcement authority to the appropriate sectoral regulator. For credit unions, the National Credit Union Administration (NCUA) should be the sole regulator.
4. A safe harbor from liability for businesses that takes reasonable measures to comply with the privacy standards.
5. Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.
6. Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.

Moreover, the Proposed Regulations do not address the numerous compliance issues present in the CCPA. Instead, the Proposed Regulations impose varying procedural requirements for a covered “business”,¹ which could include credit unions to follow when making disclosures or handling consumer requests, or complying with the anti-discrimination provisions of the CCPA.² In particular, the Proposed Regulations provide procedures for notice of right to opt-out for the sale of personal information (PI).³ Because credit unions generally do not sell PI, they should not be impacted by the opt-out requirements. Nonetheless, the implementing regulations of the CCPA should clarify the definition of “sale” so that credit unions have a clear interpretation of CCPA compliance requirements. Moreover, the Proposed Regulations fail to address interpretations of unresolved issues, which must be clarified so organizations can work towards compliance, such as the various exemptions contained in the CCPA.

Exemptions Under the CCPA

Despite the CCPA’s failure to offer exemptions that apply to organizations, NAFCU maintains the position that the CCPA should not apply to credit unions. In the alternative, the California Attorney General should establish implementing regulations that clarify that the requirements of the CCPA and its implementing regulations do not apply to organizations that solely collect GLBA-covered

¹ Section 1798.140(c) of the CCPA.

² See, Sections 999.312, 999.336 and 999.337 of the Proposed Regulations.

³ See, Section 999.306 of the Proposed Regulations.

information. Further, implementing regulations should clarify that organizations subject to the GLBA that collect CCPA-covered information should be able to comply through a regulatory regime that works in tandem with the GLBA, rather than an entirely separate, parallel framework which will be confusing for consumers and overly burdensome to credit unions.

The Proposed Regulations establish procedures for providing required notices and processing requests from consumers; however, the Proposed Regulations have not addressed a more foundational issue regarding which organizations must comply with these requirements. There is no discussion of how the various exceptions contained in the CCPA will be implemented. The CCPA provides exceptions to certain personal information already subject to state or federal regulation.⁴ These exceptions apply to types of information, not types of businesses or industries; as a result, even if a business qualifies for one of the exceptions, it will only be partially exempted for the specific types of information it collects. For credit unions, the CCPA exempts personal information subject to the California Financial Information Privacy Act (CFPA) or the GLBA.

Many credit unions only collect the personal information necessary to provide their members with the products and services they offer. In these situations, all of the information collected by these credit unions would be subject to the GLBA, qualifying for the exemption under the CCPA. It is not clear whether such a credit union would still meet the definition of a “business” in the CCPA as the credit union would not collect any “personal information” that is not excepted from the law. For credit unions in this common scenario, it is unclear whether they must comply with any of the CCPA’s requirements.

Because the Proposed Regulations do not discuss any of the CCPA exemptions, credit unions seeking to rely on the GLBA exemption, or any other partial exemptions contained in the CCPA will be forced to specifically request interpretations by the California Attorney General regarding their obligations. As a result, covered credit unions will either suffer unnecessary burden by incurring substantial costs to comply with the CCPA despite the fact that the information they collect is exempt or be forced to request and wait for duplicative clarifications from the California Attorney General’s office. NAFCU opposes the application of these requirements to information that credit unions collect that is already subject to the CFPA or the GLBA.

The implementing regulations for the CCPA need to clarify existing exemptions under the CCPA statute. Specifically, for financial institutions, the implementing regulations should recognize the CCPA’s exemption for information collected pursuant to the GLBA and clarify how it applies to covered financial institutions. This guidance should separately address compliance for credit unions that do and do not additionally collect information that falls outside of the GLBA’s scope.

The Notification Process of a Consumer’s Rights

The Proposed Regulations do not establish sufficient rules and procedures for compliance with the CCPA’s notice provisions. The privacy policy and notice requirements under the Proposed Regulations create confusion and additional burdens for covered credit unions and their members

⁴ See e.g., Section 1798.145(e) of the CCPA.

because the Proposed Regulations: (1) do not address the exceptions for financial institutions under the GLBA, and (2) create multiple notice requirements for information they presently provide under the GLBA.

Disclosure Requirements

The disclosures under the Proposed Regulations would require covered credit unions to provide detailed notice about the information collected on consumers. Credit unions are already subject to federal privacy laws such as the GLBA and have processes in place to inform consumers about the sharing of their data. Under the GLBA, a credit union is already subject to the following privacy requirements:

- Must provide initial and annual notice of its privacy policies to its customers, both members and nonmembers, and any other consumer if his or her data will be shared with nonaffiliated third parties; and
- Must allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure occurs outside of certain exceptions in the regulations.

Despite the fact that credit unions already provide detailed notice under the GLBA, Article 2 of the Proposed Regulations imposes an expanded disclosure requirement regarding information collection and privacy policies.⁵ The Proposed Regulations do not offer any clarification as to how a credit union which is covered by GLBA that still collects information outside of the GLBA's scope should reconcile the detailed privacy notice required by that law with the additional, detailed notice required by the CCPA. Only information that is not already subject to the GLBA is covered by these notice provisions in the CCPA, therefore, it would appear that a credit union would be in compliance if it were to draft a Privacy Policy that only covered the information that falls outside of the GLBA. However, such a policy could hardly be called a comprehensive description of the credit union's privacy policies. As written, the proposed regulations do not give proper effect to the GLBA exemption in the CCPA and create notice and disclosure requirements that are confusing and ambiguous and will not serve to give consumers easily understandable information.

The CCPA allows the California Attorney General to add "any exceptions necessary" to ensure that notices provided to consumers are easily understood.⁶ The Proposed Regulations should exempt credit unions subject to the GLBA from further disclosure requirements if they are in compliance with the GLBA and their existing annual privacy notice is posted on the credit union's website. The distinction between GLBA-covered information and CCPA-covered information is not one that consumers will instinctively identify and providing consumers with multiple, detailed privacy disclosures will only be confusing and frustrating for them.

If the California Attorney General is not willing to provide an exception for these credit unions, it must provide guidance as to how these credit unions can comply without requiring duplicative

⁵ Section 999.305(b) of the Proposed Regulations.

⁶ Section 1798.185(a)(6) of the CCPA.

notices or unnecessarily burdening the credit union industry. For credit unions already providing detailed privacy policy disclosures, such a requirement should make reference to the inclusion or addition of information to existing notices, rather than requiring separate, free-standing disclosures which will only serve to confuse consumers and place unnecessary compliance burden on credit unions. A separate, free-standing notice would require covered businesses to undertake a separate and new disclosure process, creating additional compliance burdens for entities, like credit unions, that already have to provide privacy disclosures to consumers under the rule.

Moreover, the Proposed Regulations include several subcategories of privacy notices that a business must provide, including notice that must be provided regarding the right of a consumer to “opt-out” of the *sale* of PI.⁷ The CCPA exempts from its definition of “sale” the processing of PI in certain specific contexts; however, these exemptions are ambiguous and could likely lead to confusion and higher compliance costs. The Proposed Regulations do not clarify the ambiguities of the definition of “sale” under the CCPA. Although, many credit unions do not “sell” member data information and would not have to comply with the notice requirements for sale of information under the CCPA, those credit unions seeking to rely on the several exemptions would benefit from additional clarification on their operation and application, including on the definition of “sale.” Providing such clarification through implementing regulations would allow businesses to rely on clear exceptions they are entitled to under the law, while reducing the risk of erroneous uses of the exceptions.

Handling Consumer Requests

The Proposed Regulations’ designated methods for receiving requests is overly prescriptive and not appropriately tailored to the reality of current online systems utilized by businesses. These requirements for methods to submit a request to know or a request to opt-out include a mandatory interactive webform. For requests to opt out, this webform must be accessed through a link entitled “Do Not Sell My Personal Information,” or “Do Not Sell My Info” on the business’s website or mobile application.⁸ Additionally, the Proposed Regulations requires businesses who collect information online to include mandatory user-enabled privacy controls, such as a browser plugin or privacy setting for opt-out of the sale of information collected.⁹

These mandatory, technical requirements for online mechanisms may be appropriate for large technology firms and multinational organizations; however, they are not appropriate for smaller organizations like credit unions. The provision would require a significant number of credit unions to do a complete overhaul of their online or mobile banking platform to include an “interactive webform via the website or mobile application” or “user-enabled privacy controls.” Many credit unions have internally developed their online and mobile banking platforms, so such an overhaul would require substantial time and resources and likely disrupt these services for members.

NAFCU is generally opposed to prescriptive technological requirements as opposed to flexible parameters that allow credit unions to choose what works best for their membership and is within

⁷ Section 999.305(a)(4) of the Proposed Regulations.

⁸ Section 999.305 of the Proposed Regulations.

⁹ *Id.*

their budget. Credit unions, as not-for-profit, member-owned financial institutions have very limited resources to make such drastic changes to their digital platforms. NAFCU strongly objects to this portion of the Proposed Regulations.

Further, regarding requests to opt-out, credit unions are already required by the GLBA to provide an opportunity to opt-out of having a consumer's information shared with nonaffiliated third parties. It would be easiest and most streamlined for consumers to make an opt-out request for the sharing or sale of their information at the same time, rather than making such a request at one time and method for GLBA-covered information and at a separate time and method for non-GLBA covered information. It would be less confusing for consumers and less burdensome on credit unions if GLBA-covered institutions could offer the opt-out of sale at the same time and in the same manner as is provided for in the GLBA.

Non-Discrimination Requirements

The Proposed Regulations' anti-discrimination provisions prohibit a business from discriminating against a consumer because they exercise their rights under the CCPA, including denying goods or services, charging different prices or rates, and providing a different level or quality of goods or services.¹⁰ Specifically, the text of the Proposed Regulations require a business to quantify and justify a price differentiation to support that the differing pricing is not a result of consumers exercising or not exercising CCPA rights but rather reasonably related to the value of the data.¹¹ Credit unions often offer differential pricing for a variety of reasons. Where credit unions collect information beyond what is necessary to offer a good or service to a member, it is often for the purpose of internal marketing, rather than for external sale.

Credit unions that choose to offer differential pricing for the purposes of obtaining information for internal marketing would face undue burden and associated costs to comply with this requirement, including additional research, learning a new market, and obtaining third-party valuations of data being used internally. The requirement of calculating the value of consumer data for differential pricing should not apply where data would only be used internally and with a consumer's informed consent. As such, NAFCU requests that the implementation regulations of the CCPA provide an exception for differential pricing in connection with data that is collected for internal purposes.

Extension of Moratorium

NAFCU understands that, per statute, the CCPA becomes operative on January 1, 2020 and there is a moratorium on enforcement by the Attorney General until the earlier of six months after the publication of the final regulations or July 1, 2020. However, given ambiguities in the law, the need for additional guidance and the significant difficulties associated with reconciling the requirements for GLBA-covered entities, coupled with the need to develop procedures and update disclosures for the new consumer rights (which cannot commence until the regulations are finalized), warrants a delay in enforcement. Although NAFCU objects to the applicability of the

¹⁰ Sections 999.301 and 1798.125 of the Proposed Regulations.

¹¹ Sections 999.307(b)(5) and 999.308(b)(4) of the Proposed Regulations.

CCPA to credit unions, NAFCU and its member credit unions request an additional delay in enforcement actions by the California Attorney General¹² to help ease the burden of compliance.

Conclusion

NAFCU appreciates the efforts of the California Department of Justice to gather substantive feedback on the Proposed Regulations but opposes the applicability of the CCPA to credit unions. Credit unions are already subject to the GLBA and take great care to safeguard the integrity of their members' personal data and provide notice regarding the sharing of that data. NAFCU cannot support varying state data privacy laws that add potentially conflicting and unnecessary burdens on credit unions. The CCPA and the Proposed Regulations add new obligations and varying standards for compliance that would create mounting and unrealistic compliance obligations for credit unions and confusion for consumers. Moreover, the Proposed Regulations do not address the variety of exceptions under the CCPA statute, including exceptions under the GLBA. Credit unions want to continue to protect their members by following the robust privacy requirements set forth in the GLBA. Ultimately, a comprehensive federal data privacy law that preempts all state privacy laws would better protect consumers and provide more certainty for credit unions.

Sincerely,



Mahlet Makonnen
Regulatory Affairs Counsel

¹² Section 1798.185(c) of the CCPA.

Message

From: Jodie Applewhite [REDACTED]
Sent: 12/6/2019 7:34:57 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: National Apartment Association Comments Regarding the Proposed California Consumer Privacy Act Regulations
Attachments: NAA Comments on CCPA.pdf

On behalf of the National Apartment Association (NAA), we respectfully submit the attached comments on the proposed regulations concerning the California Consumer Privacy Act (CCPA).

If you have any questions or comments regarding the attached letter, please do not hesitate to reach out to NAA's Vice President of Legal Affairs and Counsel, Scot Haislip, at [REDACTED]

Regards,
Jodie Applewhite

Jodie Applewhite
Manager, Public Policy



National Apartment Association
4300 Wilson Blvd., Ste. 800, Arlington, VA 22203
t: [REDACTED] f: [REDACTED]
[REDACTED] | www.naahq.org



4300 Wilson Blvd., Ste. 800
Arlington, VA 22203
703-518-6141
www.naahq.org

December 6, 2019

[(via email PrivacyRegulations@doj.ca.gov)]

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

RE: National Apartment Association Comments Regarding the Proposed
California Consumer Privacy Act Regulations

Dear Attorney General Becerra:

The National Apartment Association ("NAA") is the leading voice for the rental housing industry and we serve as a trusted partner and advocate for our members and affiliates operating in California.

NAA, on behalf of its members, writes to you to provide our comments on the proposed California Consumer Privacy Act ("CCPA") regulations (the "**Regulations**") based on our detailed review and analysis of how the Regulations, as currently drafted, would impact our members and the rental housing industry. Below we provide our detailed comments, which include recommended alternatives that we believe meet the requirements of the CCPA, while allowing our members and the rental housing industry to implement appropriate compliance solutions that benefit the consumers they serve.

Responding to Consumer Requests

We recommend responses to consumer requests to access information be limited to providing consumers with the categories of personal information we collect about that particular consumer rather than the specific pieces of information in order to provide for a more secure and safe, while equally transparent, approach to compliance. We note that the current Regulations acknowledge the potential risks of providing specific information in certain contexts in section **999.313(c)(4)**, which provides:

A business shall not at any time disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers.

We applaud the Attorney General's awareness of, and attempt to address, the risk of disclosing specific information in response to requests to access under the CCPA. We recommend that these protective measures for consumers be expanded further by allowing businesses responding to requests to access to provide only the categories of

information collected about that specific consumer, as opposed to specific pieces of information. This approach will be more secure, timelier, more straightforward, and will not reduce or limit the consumer benefits of the CCPA.

Responding to the request to access with specific pieces of information includes heightened risk should the information be obtained by an unintended or nefarious third party. Whether this risk is a substantial, articulable, and unreasonable risk (**999.313(c)(3)**) is debatable and would depend on the specifics of the request, but what is not debatable is that providing consumers with categories of information presents less risk than providing consumers with specific pieces of information. Further, to the extent a consumer wishes to verify that the business maintains accurate information about that consumer, the Regulations could provide for a way for the consumer to provide updated information to the business in order for the business to verify that its records are updated with accurate personal information. These minor changes to the Regulations would significantly enhance the security of consumer personal information, while maintaining the transparency demanded by the CCPA, as well as empowering the consumer to verify that accurate information is maintained.

B2B Exception and Service Providers

NAA recommends that the Regulations are updated to provide more details and examples regarding the applicability of the exception set out in CCPA section **1798.145(o)** ("**B2B Exception**"), which applies to personal information disclosed within the context of providing products or services to consumers where the consumer is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

Our concern here arises from the multitude of site-level contracts necessary in the apartment rental context (e.g., cleaning, maintenance, exterminator, etc.) that are often signed by individuals on behalf of the rental property owners. We recommend that the Regulations expressly include these types of personal information collections within the B2B Exception, as they are done in the context of the provision of services by one entity to another, rather than in the context of collecting personal information about the consumer themselves.

Similar to the point above, we note that section **999.314(c)** prohibits service providers from using personal information collected from one customer for the benefit of any other customer. To the extent that the B2B Exception does not apply to such providers, there is a concern that this restriction unnecessarily restricts a service providers' ability to perform important analytics that help improve the products and services offered to apartment complexes. Many apartment complexes rely on the same set of service providers and would benefit from such service providers optimizing their services for the

property owner and the consumers renting the properties based on data collected from each apartment complex (e.g., cleaners optimizing cleaning routes based on analytics performed on cleaning routes at several locations). As such, we recommend the restrictions in section **999.314(c)** be updated to provide that service providers may use personal information collected from or about customers for analytical purposes to improve their services, provided that service providers do not sell or use the personal information for any other purpose, or as otherwise permitted by the CCPA. This allows consumer personal information to continue to be protected from misuse, while also allowing for increased efficiencies and services that benefit the consumer.

Self-Reporting Consumer Requests Metrics

We note that the self-reporting requirement is a new requirement under the Regulations and is not specifically included in the text of the CCPA. While our members are compliance-minded, considering the onerous record-keeping requirements that this would impose without a clear benefit to consumers, combined with this element not having been included in the legislative intent as provided by the CCPA, we recommend the self-reporting requirements in section **999.317(g)** be removed or, at a minimum, be updated to include a carve out for businesses whose revenue is primarily derived from the "sale" of personal information.

Our concern with the self-reporting requirement as drafted is that it would require large apartment complex groups (those that process the personal data of over 4,000,000 Californians) to self-report statistics regarding how those complexes respond to consumer rights requests. Such self-reporting would require extensive documentation and record keeping that does not provide any meaningful benefit to consumers, while it imposes a tremendous cost on our members. Those resources would be better allocated to ensuring that personnel receive appropriate training to respond to the requests and ensuring that appropriate systems and capabilities are in place to provide consumers with meaningful responses. Therefore, we recommend this new requirement presented by the Regulations should be removed, or at the very least, be updated to include a carve out for businesses that do not derive 50 percent or more of their annual revenue from selling consumers' personal information.

Data Retention

The new record retention requirements imposed by section **999.317(b)** of the Regulations, which requires businesses to maintain a record of their response to every CCPA request for 24 months, are unnecessarily long and onerous, without providing any clear benefit to consumers. Consumers are already in a good position to know how a business responded to their requests and businesses may make reasonable determinations based on existing record retention requirements as to how long to maintain such records. A 24-month record retention requirement will increase businesses' costs and divert personnel time to activities that do not provide any value or

benefit to consumers. As such, we recommend removing this requirement or reducing the period to a more reasonable period, such as 6 months.

We further recommend that the limited exception related to implementing deletion requests in back-up or archival databases provided by section **999.313(d)(3)** of the Regulations be clarified to expressly exempt the back-ups or archived databases from such deletion requests. The purpose of back-ups or archived databases is to provide a clean record that would allow the restoration of a system or database in the event of a catastrophic event occurring to the live data (e.g., a ransomware attack). Requiring that deletion requests be implemented onto the back-ups or archived databases themselves upon them being accessed or restored (rather than being re-introduced into the live database or system, once it is fully restored utilizing the data from the back-up or archived database), defeats the purpose of the back-ups and, more importantly, ignores the technological limitations that exist with making specific changes to data within a back-up or archived database.

Notice Requirements

NAA recommends the notice requirements in section **999.305** be updated to provide clarity for complex situations in which there can be multiple points of collection of information from consumers. For example, a potential tenant touring an apartment complex might provide personal information when calling to schedule a tour, provide a driver's license to a security guard upon arrival, and provide financial information to a leasing agent upon a tour's completion. Requiring separate specific disclosures (i.e., a "notice at or before collection"), beyond making the privacy policy available, at all three points of collection would create excessive disclosure and potential confusion for the consumer. Therefore, we recommend updating section **999.305** of the Regulations to reflect that businesses may comply with the notice at collection requirements by making a comprehensive privacy policy available to consumers on their website or on-site where the business may collect personal information. This will provide for greater consistency in notices to consumers and reduce confusion.

Authorized Agents

We note that the text of CCPA and the Regulations include different requirements with respect to authorized agents. Under CCPA, consumer's use of authorized agents is limited to requests to opt-out of the sale of the consumer's personal information (section **1798.135(c)**); however, the Regulations note that a consumer may use an authorized agent to submit a request to know or a request to delete (**999.326(a)**). We believe expansion of the use of an authorized agent to right to know and right to delete requests is not in line with the legislative intent of the CCPA, complicates the compliance process substantially, and adds significant and unnecessary risk that the consumer information falls into the wrong hands. As such, we recommend the Regulations be updated to, consistent with the text of CCPA, limit the use of authorized agents to requests to opt-out of the sale of personal information where the potential risks to consumers are negligible.



4300 Wilson Blvd., Ste. 800
Arlington, VA 22203
703-518-6141
www.naahq.org

Conclusion

We appreciate the Attorney General's review and consideration of our comments and concerns in this letter. For any questions or feedback, please contact NAA's Vice President of Legal Affairs and Counsel, Scot Haislip, at [REDACTED]. Thank you for the opportunity to provide the rental housing industry's views for consideration in the rulemaking process. We look forward to working with you to address the concerns outlined in this letter.

Sincerely,

A handwritten signature in black ink, appearing to read 'Robert Pinnegar', with a long horizontal line extending to the right.

Robert Pinnegar
President and Chief Executive Officer
National Apartment Association

Message

From: Bankston, Kaylee Cox [REDACTED]
Sent: 12/6/2019 11:01:26 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Kevin Donnelly [REDACTED]; Julianne B. Goodfellow [REDACTED]; Lashway, Scott [REDACTED]; Clay, Delilah [REDACTED]
Subject: National Multifamily Housing Council Comments Regarding Proposed CCPA Regulations
Attachments: NMHC Comments Regarding Proposed CCPA Regulations (12.06.2019).PDF

On behalf of the National Multifamily Housing Council, we submit for your consideration the attached comments regarding the proposed California Consumer Privacy Act Regulations. Please do not hesitate to contact us should you have any questions or need additional information.

Thank you,

Kaylee Cox Bankston
Counsel

Manatt, Phelps & Phillips, LLP
Washington Square
1050 Connecticut Avenue, NW, Suite 600
Washington, D.C. 20036

D [REDACTED] M [REDACTED]
[REDACTED]

manatt.com

CONFIDENTIALITY NOTICE: This e-mail transmission, and any documents, files or previous e-mail messages attached to it, may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this message is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify us by reply email and destroy the original transmission and its attachments without reading them or saving them to disk. Thank you.

December 6, 2019

(via email PrivacyRegulations@doj.ca.gov)

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

**RE: National Multifamily Housing Council Comments
Regarding the Proposed California Consumer Privacy Act Regulations**

Dear Attorney General Becerra:

The National Multifamily Housing Council (“NMHC”) submits the following comments to the proposed California Consumer Privacy Act Regulations issued on October 10, 2019 (“Proposed Regulations”).

INTRODUCTION

Based in Washington, D.C., NMHC is a national nonprofit association that represents the leadership of the apartment industry. Our members¹ include ownership, development, management, and finance entities who help create thriving communities by providing apartment homes for 40 million Americans. NMHC members own, develop, and manage apartment communities with more than five (5) units that range in product type from garden style communities to mid- and high-rise properties. NMHC members work to house Americans across all income levels by developing and managing properties that include affordable, student, senior, workforce, military, and luxury rental housing and contribute \$3.4 trillion annually to the economy. In California, apartments and their residents contribute \$499.1 billion to the state economy annually, supporting 2.1 million jobs. This includes \$455.5 billion in local spending from California’s residents. Almost 15 percent of the nation’s entire apartment stock is located in the state of California. The following data underscores the apartment industry’s importance in the U.S. consumer economy.

- 19.5 million U.S. households live in an apartment home (renter-occupied unit in a structure with five units or more). That is 44.6 percent of all renter-occupied households and 16.1 percent of all households.²
- Approximately 43.8 million U.S. households rent their housing (whether in an apartment home or single-family home). This is 36.1 percent of all households.³

¹ The comments made herein are attributed only to NMHC and not to any individual NMHC member.

² 2017 American Community Survey 1-Year Estimates, US Census Bureau, “Tenure by Units in Structure”

³ 2017 American Community Survey, 1-Year Estimates, US Census Bureau “Tenure”

- Upwards of 108 million people, over one third of all Americans (34.0 percent),⁴ live in rental homes (whether in an apartment home or single-family home).

INDUSTRY BACKGROUND

The multifamily industry faces booming demand for rental housing, which is being driven by a fundamental shift in our nation's housing dynamics as changing demographics and lifestyle preferences have driven more people away from the typical suburban house and toward the convenience of renting. This demand is fueled by a growing population, demand for rental housing by younger Americans, immigration trends, and Baby Boomers and "empty nesters" trading in single-family houses for apartments.

At the core of the industry is a focus on service to residents and a commitment to provide a safe and secure community for them to call home. That commitment extends to ensuring that information collected, used, or retained on apartment residents is secure and their privacy is safeguarded.

The lifecycle of consumer engagement in the apartment industry typically begins when an individual explores moving into a multifamily community. As the relationship between the renter and the apartment manager may span years, industry participants collect various types of information, some on a static basis, such as during initial resident screening in the leasing process, and some continuously, such as via rental and utilities payments or other interactions. The industry is somewhat unique in that its collection of information on consumers includes dynamic and non-traditional data types in order to provide quality housing to residents and enhance their living experience. Consumer data contained in screening reports and data generated regularly and held by property managers and their service providers is crucial in accounting for rental history, tenure, and payment data, which makes up an important part of a resident's profile and can serve as a tool to improve a resident's housing opportunities in the future. It is important to note for regulators and policymakers that the absence of such data could have unintended consequences for consumers.

The emergence and popularity of smart home and building technologies is changing how the multifamily industry designs and develops properties and how apartment firms are working to meet resident demand and expectation for new technologies and amenities. Given the inherent diversity in the nation's rental housing stock, deployment and management of these new technologies can vary significantly from property to property. For example, some rental housing providers offer a white-glove experience of several connected devices, ranging from smart thermostats to voice-activated devices, that are fully managed and maintained by the apartment firm. Others have chosen to offer these technologies as an amenity and instead give residents full control and management over these technologies, including connecting the devices to residents' own personal network.

In many cases, properties of all types are deploying smart building technologies that are revolutionizing operations and lowering the cost of providing housing. Apartment firms are

⁴ 2017 American Community Survey, 1-Year Estimates, US Census Bureau "Total Population in Occupied Housing Units by Tenure"

implementing these devices to meet resident demand, increase the convenience of apartment living, and to create environmental and operational efficiencies. It is important to note that residents are demanding smart home technologies for many of these same reasons, including to improve the quality of their living experience, to reduce environmental impact, and to save money (*e.g.*, on utilities). The importance or desirability of smart home technology is only expected to increase in the future.⁵ It is clear that resident preferences and the environmental, security, and financial benefits for both residents and apartment operators from these devices ensure that their deployment will continue to drive innovation in the multifamily industry.

The use of these devices in a multifamily context as opposed to use and deployment by an individual homeowner provides for unique security and privacy considerations that apartment firms take seriously. These technologies and the nature of the information exchanged create nuanced challenges and complexities for the industry in addressing the requirements in the Proposed Regulations. By way of example, the use of smart home technologies could result in the collection of certain data types that potentially could be considered personal information under the California Consumer Privacy Act (“CCPA”), but would differ significantly from traditional types of personal information, both in the type of information generated and the way in which it is transmitted and stored. Relatedly, certain data may be maintained in unstructured formats not conducive to being readily accessed or deleted.

These factors introduce unique complexities to the multifamily industry in complying with the Proposed Regulations as currently drafted. NMHC believes that the Proposed Regulations inadvertently create new risks to the privacy and security of consumer data. For example, the Proposed Regulations contemplate significant transmissions of personal information that would otherwise remain stored, which inherently creates privacy and security risks to consumers. NMHC believes many of these challenges can be addressed through clarifications and amendments to the Proposed Regulations. NMHC proposes that, to the extent possible, the California Government consider minimizing all scenarios where additional transmissions of personal information would be required in an effort to mitigate privacy and security risks to consumers. In addition to comments on specific sections set forth herein, NMHC believes the industry also would benefit from additional clarification and guidance in the Proposed Regulations around use cases that would constitute a “sale” of personal information as well as exceptions to deletion requests related to “internal uses,” as contemplated by the CCPA.

As noted above, the privacy and security of consumers’ information is of utmost importance to NMHC and its members. The comments set forth herein are intended to aid the Attorney General in further refining the CCPA regulations in an effort to better protect the privacy and security of consumers and streamline procedures to enable businesses’ compliance with the law.

⁵ According to the “2020 NMHC/Kingsley Renter Preferences Report,” 44 percent of respondents indicated having five (5) or more Internet-connected devices and of those aged 18-34, half (50%) indicated having five (5) or more Internet-connected devices. Even further, 72.3% of respondents were interested in smart lighting; 66.8% interested in smart locks; 77.1% interested in smart thermostats, and 71.6% interested in a video doorbell. The report highlights survey results from 372,000 apartment residents nationwide, the largest ever in history, covering leasing decision factors, amenity desires, and the like. 2020 NMHC/Kingsley Resident Preferences Report, <https://www.nmhc.org/research-insight/research-report/nmhc-kingsley-apartment-resident-preferences-report/>.

COMMENTS REGARDING PROPOSED REGULATIONS

I. VERIFICATION PROCESS

The following sets forth NMHC's comments related to the verification requirements in Article 4 regarding (1) the general rules for verification; (2) the process for requests that cannot be verified; (3) the verification of requests made by authorized agents; and (4) privacy policy disclosures related to the verification process.

A. Verification of Requests – General Rules

The following sets forth NMHC's comments regarding the general rules for the verification process.

1. Proposed Regulations: Article 4, §§ 999.323-325

Article 4 of the Proposed Regulations requires businesses to establish, document, and comply with a "reasonable method" for verifying consumer requests; however, the Proposed Regulations offer little guidance as to what may constitute a "reasonable method."

2. NMHC Request and Recommendation

NMHC seeks further clarification as to "reasonable" verification methods. NMHC does not seek a prescriptive methodology for the verification process; rather, NMHC asks that the Proposed Regulations be amended to provide examples of verification methods that would be considered "reasonable" while permitting businesses to implement other methods at their discretion.

Further, NMHC recommends that the Proposed Regulations be amended to provide for a safe harbor from liability for businesses that follow a reasonable verification method.

3. Additional Analysis

As noted above, the Proposed Regulations do not provide specific guidance as to what would qualify as a "reasonable" verification method. Relatedly, as NMHC currently understands the Proposed Regulations, portions of Article 4 appear to be in conflict with other provisions of the Proposed Regulations. For example, section 999.323(b)(3)(a) instructs businesses to consider the sensitivity of personal information in implementing the verification process and that "[s]ensitive or valuable personal information shall warrant a more stringent verification process." However, section 999.313(c)(3) prohibits the disclosure of personal information that would create a substantial, articulable, and unreasonable risk. Section 999.323(b)(3)(a) also designates certain types of personal information as "presumptively sensitive," which are prohibited from disclosure pursuant to section 999.313(c)(4) (*e.g.*, Social Security number; driver's license number). The Proposed Regulations seem to suggest that businesses should implement stringent verification methods to disclose sensitive personal information (Section 999.323), while at the same time, the Proposed Regulations prohibit the disclosure of sensitive personal information (Section 999.313). Additional guidance on these topics would be beneficial to ensure compliance with the requirements and to protect the privacy and security of consumers.

NMHC believes this potential conflict can be rectified by amending the Proposed Regulations to (1) provide additional guidance as to what constitutes reasonable verification measures; and (2) eliminate the requirement that businesses provide specific pieces of personal information in response to access requests (as discussed in further detail in comments in section (II)(C) below).

B. Process for Requests that Cannot be Verified

The following sets forth NMHC's comments related to the process for requests that cannot be verified.

1. Proposed Regulations: Article 4, §§ 999.323-325

While Article 4 of the Proposed Regulations addresses, in part, a business's obligations when a request cannot be verified, NMHC believes further clarification is needed to protect consumers against fraudulent requests.

Relatedly, section 999.324(b) states that, if fraudulent or malicious activity is suspected, a business shall not comply with a request *until* the business can verify the request. NMHC is concerned that the current language implies a business is obligated to continually attempt to verify a request, without limitation, which could be unreasonable and unduly burdensome on businesses.

2. NMHC Request and Recommendation

NMHC seeks further clarification as to businesses' obligations where a request for access or deletion is denied because the consumer's identity cannot be verified through the verification process. Specifically, NMHC would like confirmation as to whether a consumer is entitled to attempt to rectify a request that was denied on verification grounds, and if so, what limitations may apply.

In addition, due to the security concerns presented by potential fraudulent requests or requests where a consumer's identity cannot be verified, NMHC recommends that the Proposed Regulations be amended to make clear that, where a business denies a request from a consumer on verification grounds, such consumer must wait 90 days, or some other additional period of time, before initiating another request, and the business is not obligated to respond to any requests purportedly received from that consumer before that time period is complete.

Finally, NMHC recommends the language in section 999.324(b) be amended as follows:

999.324(b)

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete ~~unless until further~~ verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer. A business shall not be obligated to comply with a consumer's request to know or request to delete where the business has followed its verification procedures and is not able to verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

C. Verification of Requests – Authorized Agent

The following sets forth NMHC's comments related to the verification of requests made by authorized agents.

1. Proposed Regulations: § 999.326

Section 999.326 would permit an authorized agent to submit requests to know or requests to delete on behalf of a consumer. Without further direction as to verification requirements related to an authorized agent, NMHC believes the current proposed provision creates both privacy and security risks to consumers.

2. NMHC Request and Recommendation

NMHC recommends that the Proposed Regulations be amended to permit an authorized agent to act on behalf of a consumer only in the context of consumers' right to opt-out of the sale of their personal information and to require consumers to submit requests to know and requests to delete directly.

If the above change is not made, NMHC recommends in the alternative that the Proposed Regulations be amended: (1) to provide further guidance for verifying the identity and authority of authorized agents; (2) to permit businesses to confirm with a consumer directly that an authorized agent is authorized to act on their behalf; and (3) to provide a safe harbor from liability for businesses that follow the verification process.

Finally, NMHC proposes that the time period to respond to requests made by authorized agents be extended to 90 days and provide for an additional 90 day extension where necessary.

3. Additional Analysis

As noted above, NMHC believes allowing authorized agents to submit requests to know and requests to delete creates privacy and security risks to consumers. NMHC believes this risk is further heightened in the multifamily industry. As discussed above, apartment owners and managers collect various types of information on residents in order to operate and maintain apartment communities. The nature of this information differs substantially from, for example, information an online retailer may collect about its customers.

As a result, NMHC believes the risk of fraudulent authorized agent requests is not only higher in the multifamily industry, but also creates more serious risk to consumers than in other business contexts. For example, a nefarious actor could attempt to use the authorized agent process as a means to get sensitive information about residents, such as information pertaining to their living habits or lifestyle, all of which could present risk beyond identity theft—especially if the obligation to confirm specific personal information remains in the Proposed Regulations. In extreme cases, a bad actor who fraudulently obtained information about a resident could create physical security risks to consumers. NMHC member firms consider the safety and security of their residents to be of utmost importance and are concerned about the unintended consequences created by sharing sensitive data under the Proposed Regulations.

Further, given the importance of verifying that an authorized agent in fact has the authority to make requests on behalf of a consumer, the verification process for an authorized agent likely will require additional time than for consumers making requests directly. For example, a business may desire or need to obtain notarized documents, such as an affidavit, from both the agent and the consumer as part of the verification process to help protect against fraudulent requests. In the event the Proposed Regulations are not amended to limit authorized agent requests to only a consumer's opt-out right, increasing the time period to respond to requests made by authorized agents will further protect the privacy and security interests of all consumers.

D. Privacy Policy – Description of Verification Process

The following sets forth NMHC's comments regarding privacy policy disclosures related to the verification process.

1. Proposed Regulations: § 999.308(b)(1)(c)

Proposed Regulation section 999.308(b)(1)(c) requires that a privacy policy “[d]escribe the process the business will use to verify the consumer request, including any information the consumer must provide.” While NMHC agrees that a verification process is necessary, NMHC believes the requirement to describe in detail the verification process, on a business's public website, potentially creates security risks to consumers that significantly outweigh any potential interest consumers may have in such information being publicly available in the business's privacy policy.

2. NMHC Request and Recommendation

To further protect consumers against fraudulent requests, NMHC proposes amending section 999.308(b)(1)(c) as follows:

999.308(b)(1)(c)

- c. Disclose that the business will require the consumer to verify their identity before the business may process the consumer request. ~~Describe the process the business will use to verify the consumer request, including any information the consumer must provide.~~

In the event section 999.308(b)(1)(c) is not amended as set forth above, NMHC recommends in the alternative that the following requirement be omitted:

999.308(b)(1)(c)

- c. ~~Describe the process the business will use to verify the consumer request, including any information the consumer must provide.~~

3. Additional Analysis

Requiring businesses to make the verification process publicly available could serve as a roadmap for bad actors to institute fraudulent or nefarious access or deletion requests. While NMHC recognizes that bad actors may still seek to initiate access or deletion requests, and could ascertain the verification requirements through a business's request procedures, requiring the additional step of going through the submission process would mitigate this risk.

NMHC proposes that section 999.308(b)(1)(c) be amended to require only that businesses disclose in their privacy policy that consumer requests will be subject to a verification process. Doing so will put consumers on notice that verification requirements will apply to any request, and consumers will be informed of any verification procedures at the time a request is submitted.

II. REQUESTS TO KNOW AND REQUESTS TO DELETE

The following sets forth NMHC's comments regarding requests to know and requests to delete related to (1) methods for submitting requests; (2) the timeline for responding to requests; (3) responding to requests to know; and (4) responding to requests to delete.

A. Methods for Submitting Requests

The following sets forth NMHC's comments related to methods for submitting requests to know and delete.

1. Proposed Regulations: § 999.312

As NMHC currently understands the Proposed Regulations, Section 999.312 sets forth that businesses designate at least two methods for submitting requests to know and that at least one

method must reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods. NMHC believes this requirement is overly burdensome and does not serve the best interest of the consumer.

Section 999.312(a) further requires businesses that operate a website to use an “interactive webform accessible through the business’s website or mobile application.” NMHC believes that requiring use of webforms creates unnecessary security risk to consumers as webforms are often susceptible to security flaws and vulnerabilities.

2. NMHC Request and Recommendation

NMHC recommends that Section 999.312 be amended to permit businesses more flexibility in designating the request method in order to best serve the consumer. In particular, NMHC recommends that the section be modified to require businesses to offer the following two methods: (1) one method that reflects the primary method by which the business interacts with consumers; and (2) the second method be either a toll-free phone number or a method of submitting a request electronically.

Further, NMHC recommends that Section 999.312 be amended to omit the requirement for businesses to use a webform. Instead, NMHC proposes that Section 999.312 allow for businesses to designate a method for submitting requests electronically, which may include the creation of a basic user account, by the consumer or by the business on the consumer’s behalf, for the sole purpose of implementing and completing the request process.

3. Additional Analysis

As noted above, NMHC believes consumers would benefit by permitting businesses additional flexibility in providing the method to submit consumer requests. For example, in the multifamily industry, a normal channel of communication often occurs in-person at the front desk or management office. In that case, a property management company may want to permit their residents to make requests in person (*e.g.*, via a tablet interface made available in the office, or via personnel who submit requests on residents’ behalf) for the convenience of the resident. NMHC proposes that businesses be permitted to designate the method of submitting requests, which would include the primary communication channel with consumers as well as either a phone number or electronic submission.

In addition, NMHC is concerned that the requirement to offer a webform creates security risks to consumers. Due to their open interface, webforms are also prone to spamming and bot technologies, which could flood intake channels with illegitimate requests. While NMHC recognizes that CCPA section 1798.130(a)(2) prohibits businesses from requiring a consumer to create an account in order to make a verifiable consumer request, NMHC believes the privacy and security interests of the consumer are best served if businesses are permitted to require basic user accounts for the limited purpose of implementing the consumer request. Doing so will better allow businesses to verify the identity of the consumer and enhance security controls for the request process.

B. Timeline for Responding to Requests

The following sets forth NMHC's comments related to the timeline for responding to requests to know and to delete.

1. Proposed Regulations: § 999.313(b)

Section 999.313(b) of the Proposed Regulations states that the 45-day period for a business to respond to a request to know or delete "will begin on the day that the business receives the request, regardless of time required to verify the request." NMHC believes the current language creates unnecessary time constraints that may impair businesses' ability to conduct adequately its verification process and appropriately respond to consumer requests.

2. NMHC Request and Recommendation

NMHC recommends section 999.313(b) be amended as follows:

999.313

(b) Businesses shall respond to requests to know and requests to delete within 45 days. The 45- day period will begin on the day that the business verifies ~~receives~~ the request, pursuant to the verification requirements set forth in Article 4 ~~regardless of time required to verify the request~~. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is verified ~~received~~, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

If the above language is not accepted, NMHC proposes in the alternative the following amendments:

999.313

(b) Businesses shall respond to requests to know and requests to delete within 45 days. The 45- day period will begin on the day that the business receives ~~the~~ a complete request, regardless of time required to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the complete request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

999.301

"Complete request" means a request to know or request to delete where the consumer (1) has followed a business's designated method to submit the request and (2) submitted all required documentation and/or information required by the business as part of the designated submission process, including for the verification process.

3. Additional Analysis

NMHC believes the Proposed Regulations, due to the time restrictions, may reduce businesses' ability to take appropriate steps to verify adequately consumer requests. Requiring businesses to complete a verification process and to respond to requests in a specified time period, without flexibility, can result in inadvertent errors and incomplete procedures. For example, businesses may feel the need to rush or expedite the verification process in order to meet the 45-day timeline, which could result in inaccurate or insufficient verification procedures and increase the likelihood of both fraudulent requests and inaccurate or incomplete responses to requests. Consumers' privacy and security interests will be better served if the process encourages a thorough and thoughtful verification process that is not unnecessarily rushed due to regulatory time constraints. Amending the requirement so that the 45-day period begins once a business has verified a request will ensure that businesses have the opportunity to properly conduct the verification process and better protect consumers against fraudulent requests.

C. Responding to Requests to Know

The following sets forth NMHC's comments related to responding to requests to know.

1. Proposed Regulations: § 999.313(c)

Section 999.313(c) sets forth various requirements for responding to consumer requests that seek the disclosure of specific pieces of information about the consumer. NMHC believes the security risk presented by this requirement outweighs any interest the consumer may have in obtaining specific pieces of personal information from the business.

2. NMHC Request and Recommendation

NMHC recommends the Proposed Regulations be amended to require only that businesses respond to requests to know by disclosing categories and types of personal information collected on a particular consumer instead of specific pieces of personal information, including, but not limited to, by striking section 999.313(c)(1) in its entirety. Consumers will be better served by this approach because it will minimize security risks and streamline businesses' ability to respond appropriately to consumer requests.

3. Additional Analysis

Requiring businesses to disclose specific pieces of personal information increases the likelihood that such information could be misused or compromised. The Proposed Regulations appropriately recognize the inherent security risk in requiring businesses to provide specific pieces of personal information. For example, the Proposed Regulations expressly prohibit the disclosure of certain sensitive information (*e.g.*, Social Security numbers; driver's license numbers) as well as the disclosure of personal information that would create a "substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account... or the security of the business's systems or networks." *See* § 999.313(c)(3)-(4). The Proposed Regulations also require that businesses use "reasonable security measures" in the transmission of personal information to the consumer. *See* § 999.313(c)(6).

Rather than placing the burden on businesses to demonstrate in each case that providing certain personal information would create a substantial, articulable, and unreasonable risk, such risk can be eliminated through the regulations by requiring only that businesses disclose the categories and types of personal information. Doing so will not reduce or limit the consumer benefits of the CCPA as consumers will still have access to individualized categories and types of personal information that a business collects on them pursuant to Proposed Regulations section 999.313(c)(9)-(11).

In addition, requiring businesses to provide specific pieces of information creates inefficiencies in the response process as significant time would be required to identify and provide the individualized data for consumers. The requirement presents unique challenges to the multifamily industry, in particular, due to the nature of information collected, the business-to-consumer continuous relationship, and data collection between apartment residents and owners and managers, as well as the interdependencies of service providers who may collect residents' information. For example, providing specific information collected through smart home technology, to the extent the data would include CCPA personal information, would be impractical and potentially impossible, depending on the nature and format of the data. Alternatively, permitting businesses to instead disclose the general categories and types of information collected would be less burdensome for businesses and still appropriately inform the consumer as to what information is collected.

D. Responding to Requests to Delete

The following sets forth NMHC's comments related to responding to requests to delete.

1. Proposed Regulations: § 999.313(d)(3)

Section 999.313(d)(3) would permit a business to "delay compliance" with a request to delete where personal information is stored on archived or backup systems until the system is "next accessed or used." However, NMHC believes this requirement does not align with the functionality of many systems and practices.

2. NMHC Request and Recommendation

NMHC recommends that section 999.313(d)(3) be amended to provide for a complete exception to requests for deletion for personal information stored on archived or backup systems.

3. Additional Analysis

Data backups typically are not accessed on a regular basis and many are not in readily accessible formats. In the event a company needed to access backups, it is often indicative of an issue or failure with the primary systems. Moreover, the format and structure of data backups are not designed for the concept of deleting individual pieces of data (*e.g.*, backup tapes do not accommodate this function). The very purpose of a backup is to co-locate a copy of data so that it could be available to maintain business operations in the event the original data is corrupted, lost, or otherwise inaccessible. The reading of the Proposed Regulations would require a business to address an entire backup in full in order to delete specific personal information.

Doing so would create significant and unreasonable risk to the security and operation of the business, as all data on the backup would no longer be available.

III. REQUESTS TO ACCESS OR DELETE HOUSEHOLD INFORMATION

The following sets forth NMHC's comments related to requests to access or delete household information.

A. Aggregate Household Information

The following sets forth NMHC's comments related to requests for aggregate household information.

1. Proposed Regulations: § 999.318(a)

Section 999.318(a) of the Proposed Regulations would permit a consumer, without a password-protected account, to submit a request to know or request to delete as it pertains to household personal information and would obligate a business to respond by "providing aggregate household information." NMHC seeks further clarification as to this requirement.

2. NMHC Request and Recommendation

NMHC recommends that section 999.318(a) be stricken in its entirety. In the alternative, if section 999.318(a) is not deleted, NMHC seeks further clarification and guidance as to (1) what exact information businesses must provide in order to comply with the requirements, including clarification as to the definition of "aggregate household information"; and (2) the verification requirements to ensure all household members' privacy is adequately protected.

3. Additional Analysis

The term "aggregate household information" is not defined in the CCPA or the Proposed Regulations. "Aggregate consumer information," however, is defined as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, *that is not linked or reasonably linkable to any consumer or household*, including via a device." CCPA, § 1798.140(a) (emphasis added). If the intent of the Proposed Regulations is to permit individuals to access aggregate consumer information, as defined under the CCPA, doing so arguably goes beyond the requirements of the statute. Specifically, consumers' rights to request access or deletion are tied to the access or deletion of their personal information. Section 999.318(a), as proposed, seems to suggest that individuals have a right to information beyond their personal information. Further, the very definition of "aggregate consumer information" requires that the data not be reasonably linkable to any household.

Alternatively, if the intent of section 999.318(a) is to permit an individual consumer to obtain the collective categories of personal information about all consumers living in a particular household, NMHC believes this violates the privacy rights of other members in the household. This concern is particularly relevant to the multifamily industry where businesses regularly collect information on individuals living together in a household who are not necessarily

individuals of the same family or otherwise related. For example, it is common in our industry for students, military members, and other individuals to occupy a single dwelling. In fact, almost one-fifth (18 percent) of apartment households are comprised of non-family households, such as roommates.⁶ Further, even members of the same family could be at risk if only one individual is needed to make a request (*e.g.*, an estranged spouse still living in the household). Permitting an individual to obtain information on all members of the household, even information in the aggregate or general categories of personal information, would violate the privacy rights of other individuals living in the household.

As written, NMHC believes the Proposed Regulations could enable an individual to obtain sensitive information (*e.g.*, a resident's legal status) on another individual living in the household without that individual's knowledge or consent. To illustrate, consider the following scenario. Two college students occupy a household in a privately owned and managed student housing community. One student initiates a request to know as it pertains to household information. In response, the business confirms that it collects various categories of information on the household, including criminal history, which can include complaints filed against members of the household. The consumer who initiated the request has never been involved with a criminal proceeding or been made aware of any complaints filed against her. Therefore, she may be able to infer that a criminal complaint was filed related to her roommate, even without accessing the specific information related to such reports.

B. Joint Household Requests

The following sets forth NMHC's comments related to joint household requests to know and requests to delete.

1. Proposed Regulations: § 999.318(b)

The same concerns set forth above also arise with respect to section 999.318(b), which would require a business to provide specific pieces of information, or delete household personal information, in response to a joint request by a household. Although the section states the requirement is subject to the Article 4 verification requirements, NMHC believes further clarity is needed in order to protect the privacy of all individuals residing in a household.

2. NMHC Request and Recommendation

NMHC recommends that section 999.318(b) be amended to make clear that (1) each adult member of the household must authorize the access or deletion request; (2) the business must verify the identities of each adult member making the request; and (3) the business must verify that each member of the household covered by the request is currently a member of the household. Proposed language is as follows:

⁶ NMHC tabulations of 2018 American Community Survey microdata

999.318

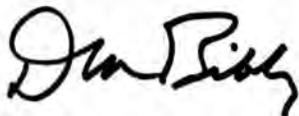
- ~~(a) Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.~~
- (b) If all consumers of the household jointly request access to ~~specific pieces~~ categories of personal information for the household or the deletion of household personal information, ~~and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4,~~ then the business shall comply with the request only if (a) the business can verify that each adult member of the household authorized the request; (b) the business can individually verify the identities of each adult member of the household making the request, subject to verification requirements set forth in Article 4; and (c) the business can verify that each member of the household to whom the request pertains is currently a member of the household.

CONCLUSION

The security and privacy of consumer information is a top priority to the multifamily industry. While the Proposed Regulations are certainly well-intentioned, NMHC believes the language as currently written inadvertently creates new risks to the privacy and security of consumer data. NMHC believes these concerns can be addressed through further amendment to the Proposed Regulations, as set forth above.

NMHC appreciates the opportunity to present the views of the multifamily industry in connection with the continued development and implementation of the CCPA. NMHC shares the same goal of protecting consumers' privacy and stands ready to work with the Attorney General to ensure the CCPA serves as an effective standard that recognizes the unique nature and needs of the rental housing industry while ensuring consumers' privacy rights are protected.

Sincerely,



Doug Bibby
President
National Multifamily Housing Council

Message

From: Bugel, Madeleine [REDACTED]
Sent: 12/6/2019 6:42:29 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: NEMA Written Comments - CCPA Proposed Regulation
Attachments: NEMA CCPA Comments 20191206.pdf

Good afternoon,

The National Electrical Manufacturers Association (NEMA), the leading trade association representing manufacturers of electrical and medical imaging equipment, provides the attached comments on the Proposed Text of Regulations for Chapter 20, California Consumer Privacy Act (CCPA) Regulations. These comments are submitted on behalf of NEMA Member companies across multiple Product Sections.

Best,
Madeleine Bugel



Madeleine Bugel

Manager

State and International Government Relations

1300 North 17th Street | Suite 900

Rosslyn, VA 22209

Office: [REDACTED]

Cell: [REDACTED]

[REDACTED]



National Electrical Manufacturers Association

The association of electrical equipment
and medical imaging manufacturers
www.nema.org

December 6, 2019

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

Re: NEMA Comments on California Consumer Privacy Act Proposed Regulations

The National Electrical Manufacturers Association (NEMA), the leading trade association representing manufacturers of electrical and medical imaging equipment, provides the attached comments on the Proposed Text of Regulations for Chapter 20, California Consumer Privacy Act (CCPA) Regulations. These comments are submitted on behalf of NEMA Member companies across multiple product Sections.

NEMA represents more than 325 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems across 56 product Sections. Our combined industries account for over 370,000 American jobs in more than 6,100 facilities covering every state. Our industry produces \$124 billion shipments of electrical equipment and medical imaging technologies per year with \$42 billion exported. In California, 68 of our Member companies maintain 181 facilities employing over 12,000 people.

The proposed CCPA regulation provides many clarifications and details. We seek further clarifications on several sections.

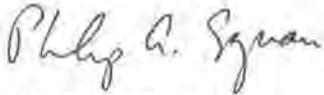
1. §999.313.(c)(3.) - The proposed regulations state that a business can decline to provide a consumer with specific personal information when there is an unreasonable risk to the security of that personal information. While a business should promptly respond to requests to identify categories of personal information held, requests to modify and/or delete “low value” personal information—such as; name, email address, or phone number—would represent a security risk that outweighs the potential benefit to the consumer. In these cases, it would be unreasonable to disclose the specific personal information. The Office of the Attorney General should be as clear as possible on this point and should provide additional guidance to the public.
2. §999.326(a)(1) – Questions remain about the extent of a business’s obligation to confirm the validity of the written permission granted from a consumer to an authorized agent for a request to know (i.e., validate the proof provided under 999.326(c)). Because the consumer will have to separately verify its identity directly with the business, any person could independently present a forged written permission document claiming to represent a verified consumer and the business will be required to disclose to the agent the consumer’s personal information. Additional guidance from the AG office is needed on this topic.
3. §999.337(b)(5)(a)—A good-faith estimate of personal data collected by a business can vary greatly and be proprietary. NEMA believes that there should be mechanisms in place to ensure the confidentiality of the estimates.
4. §999.312(a), §999.312(b), and §999.315(a)—These sections requiring businesses to have two or more designated methods for a person submitting requests to a business are overly prescriptive.

NEMA disagrees that there is any benefit to having two or more methods for these communications. Requiring more communication methods for a business to monitor may increase the risk of fraudulent data requests.

5. §999.313(c)(6) and §999.323(d)—These sections instruct businesses to use reasonable security measures when transmitting personal information and detecting fraudulent identity-verification activity. The phrase “reasonable security measure” is undefined. Industry maintains best practices for data protection which may involve compliance with internationally recognized standards development organizations (SDOs) and voluntary consensus standards.

If you have any questions or need more information, please contact Madeleine Bugel at [REDACTED] or [REDACTED]

Sincerely,



Philip A. Squair
Vice President, Government Relations

Message

From: Shanahan, Richard [REDACTED]
Sent: 12/6/2019 7:51:33 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Mizoguchi, Kenichirou [REDACTED]
Subject: Notice of Proposed Rulemaking Action Concerning California Consumer Privacy Act (CCPA)
Attachments: 12062019_CCPA AG Comments.pdf

Dear Privacy Regulations Coordinator,

Please find attached comments by Hitachi Group Companies doing business in the United States regarding rulemaking on the California Consumer Privacy Act. We look forward to working more with the Attorney General's Office to ensure California maintains its innovation ecosystem.

If you have any questions, please feel free to contact me.

Best regards,

Richard Shanahan

Manager | Government & External Relations
Hitachi, Ltd. | Washington, DC Corporate Office
t. [REDACTED] | m. [REDACTED]
[REDACTED]

Follow Us

www.hitachi.us/gov-relations

HITACHI
Inspire the Next

December 6, 2019

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

RE: Notice of Proposed Rulemaking Action Concerning California Consumer Privacy Act (CCPA)

Dear Attorney General Becerra:

The following comments are submitted by Hitachi Group companies (“Hitachi”) doing business in the United States in connection with the Notice of Proposed Rulemaking Action (NOPA) to adopt 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).

Background on Hitachi

Founded in 1910 and headquartered in Tokyo, Japan, Hitachi, Ltd. is a global technology conglomerate answering society’s most pressing challenges through cutting-edge operational technology (OT), information technology (IT), and products/systems. A Social Innovation leader, Hitachi delivers advanced technology solutions in the mobility, human life, industry, energy, and IT sectors. The company’s consolidated revenues for FY2018 (ended March 31, 2019) totaled \$86.2 billion, and its 803 companies employ 295,000+ employees worldwide.

Since establishing a regional subsidiary in the United States in 1959, Hitachi has been a committed American partner. For over thirty years, it has invested heavily in research and development (R&D) in the U.S., and this continued reinvestment has resulted in 11 major R&D centers that support high-skilled jobs in manufacturing and technology. Dedicated to delivering the technologies of tomorrow, Hitachi recently opened a Center for Innovation in Santa Clara, California to explore applications in machine learning, artificial intelligence, Internet of Things (IoT) devices, data analytics, and autonomous vehicles among other advanced technologies. Hitachi is also proud of its human capital investment, supporting 21,000 employees across 88 companies in North America. At 13% of total revenue, North America is Hitachi, Ltd.’s second largest market, generating \$10.9 billion in revenue in FY2018.

Hitachi welcomes the opportunity to engage with the California Department of Justice and commends the Attorney General (“AG”) for seeking to clarify compliance and enforcement guidelines for the CCPA. Privacy standards should be fair, equitable, and protect the public while also fostering innovation in the State of California and across the country.

Hitachi’s Approach to Privacy

Hitachi aims to co-create a human-centric society in which everyone can enjoy the benefits of digital technologies, and customer and employee privacy is central to that vision. Towards that end, we have developed and implemented a privacy-review process that includes regular, company-wide evaluations to identify insufficient practices, action plans to bolster privacy protections, and rigorous audits to ensure continuing compliance.

We also use privacy-focused training programs to make sure our critical, decision-making employees stay up-to-date on the company’s latest privacy requirements. By prioritizing privacy education in this manner, we ensure that privacy dictates our employees’ decision-making process around all forms of data. Our Information Security Risk Management Division continuously monitors changes to privacy laws across countries.

Given Hitachi’s global footprint and diverse business interests, it is imperative that we not just comply with applicable laws. Instead, we are actively cultivating an environment of trust and privacy by design.

Hitachi Vantara

2535 Augustine Drive, Santa Clara, CA 95054

www.HitachiVantara.com

Responses to NOPA

Business Threshold Requirements (Civil Code Section 1798.140, subdivision (c))

Whereas broad threshold requirements generally safeguard innovation, overly-narrow threshold requirements generally stymie it. Despite its broad parameters, Provision 1798.140 (C)(1)(A) only serves to create confusion. It cites \$25M in gross revenues, but fails to specify if that amount is to be determined only from revenues obtained through sales in California, received from California consumers, or if it is more encompassing.

For example, if a small business located outside of California has \$25M in revenue primarily from sources outside the state, yet a small portion of that revenue can be attributed to California, does it meet the definition? What about a global company that has one client in California and generates well below the \$25M threshold; is it required to follow the other provisions of CCPA or is it not defined as a California business since it does not generate \$25M from California sources?

Treatment of Households (Civil Code section 1798.140, subdivision (o))

Household is defined in 999.301(h) as a person or group of people occupying a single dwelling. This definition raises significant questions. First, who specifically holds the rights for the household; does each individual person hold their own distinct household privacy rights, or can one person speak for the entire household? In instances where persons in the dwelling are not related, what determines who can speak for the household and who could exercise the rights granted by CCPA? If there are shared devices within a household that includes non-relatives, who is assigned the personal data rights to those shared devices? Do those determined to be non-owners have rights to these shared data devices? Consider smart objects within the household that are not specifically connected to a single user's profile or a collective household profile; does the data collected by such a device constitute personal data, and if so, who in the household has ownership of that data?

It is important that the final regulations work to eliminate the ambiguity around "household" and how privacy ownership rights are conveyed or assigned.

Verification of Requests

Article 4 lays out various considerations businesses can consider when verifying a request to "Know, Delete, Opt-Out, and Opt-In After Opting-Out." The regulations, however, create gaps that do not provide certainty on liability issues such as the following:

1. If a business employs a "reasonable method" for verifying a request, is the business protected from liability if the request turns out to be fallacious?
2. If a business declines to fulfill a request because it has a good-faith belief the requestor is not verified, or if there is not enough information to reasonably verify the requestor, is the business held harmless if it turns out the request did come from a valid requestor?

Concerningly, some businesses could avoid California as a commercial market or move cutting-edge research out of the state to avoid unnecessary liability if there are not clear safe harbor provisions when a company puts into place reasonable, risk-based verification methods as generally outlined in Article 4. Small businesses in particular could find these verification methods particularly onerous. Given that, the AG would be wise to recognize a business's resources and capabilities when determining if the business has created a reasonable standard for verification.

In lieu of creating prescriptive rules regarding verification, the AG would be better served by creating a guidance document that favors a risk-based verification process that also takes into account the sensitivity of the data that is being processed. The regulations could then cite adherence to the guidance document as part of a test to create a safe harbor provision for businesses under this verification title. This would allow some flexibility as technology and security advances, and would give businesses certainty to liability under the title.

Hitachi Vantara

2535 Augustine Drive, Santa Clara, CA 95054

 www.HitachiVantara.com

Service Provider

The definition of service providers found in 1798.40(v) is specific and we appreciate the reference to constructional language requirements. However, there could be vendors or service providers who have contracts that do not meet the requirements and may have access to California consumers' personal information. To help avoid confusion with various vendor contracts, the AG should consider creating a certification form specifically allowing vendors to not be classified as service providers.

Business Outside of CA

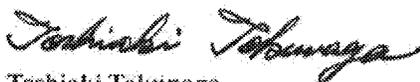
California Civil Code 1798.145(a)(6) states that the statute will not restrict a business' ability to "collect or sell a consumers personal information if every aspect of that commercial conduct takes place wholly outside of California." While clarifying language states "commercial conduct takes place wholly outside California if the business collected that information while the consumer was outside California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold," this is adding complexity as to exactly when a potential consumer was physically in the state. If a California resident is not physically in California when data is collected, is that information exempt from CCPA? Other portions of the regulations seem to intimate that merely being "domiciled" in California would subject the data to CCPA. What if that same "domiciled" person spends long periods of time in another state; is all their data subject to CCPA, or does it only apply to data generated when the consumer was physically present in the state?

When it comes to the use of website cookies, further clarification with regards to CCPA's scope is needed. Given the global nature of many corporate websites, a California resident may access a corporate website that is not designed to target California consumers. Would the corporation's use of cookies—simply to assess web traffic without any sale of that data—bring the corporation under the purview of CCPA? Is it the law's intention to cover this type of site visit even if the corporation is not marketing a product to the consumer?

Conclusion

Hitachi lauds the AG's efforts and looks forward to continuing to work with the State of California as CCPA takes effect.

Sincerely,



Toshiaki Tokunaga
Chairman of the Board
Hitachi Vantara Corporation

Hitachi Vantara

2535 Augustine Drive, Santa Clara, CA 95054

 www.HitachiVantara.com

Message

From: Dan Mustico [REDACTED]
Sent: 12/6/2019 7:45:15 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: OPEI letter on California Consumer Privacy Act
Attachments: OPEI letter re CCPA 20191205.pdf

Please accept our attached inquiry and request with respect to the CCPA. Thank you in advance.

Best regards,
Dan

Daniel J. Mustico
Vice President, Government & Market Affairs
Outdoor Power Equipment Institute, Inc.
1605 King Street, 3rd Floor
Alexandria, VA 22314
Direct: [REDACTED]
Main: (703) 549-7600
Cell: [REDACTED]
e-mail: [REDACTED]



Email Disclaimer:

Please be informed that this email and any materials attached herewith may contain confidential or legally privileged information that is intended solely for the use by its named recipient. If you have received this email in error, please notify us immediately by reply email and delete this email from your system. Any disclosure, use, copying, printing, distribution or reliance upon the contents of this email is strictly prohibited.



Transmitted via-email: PrivacyRegulations@doj.ca.gov

December 6, 2019

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

Re: Public Comments to §§ 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)

Dear Attorney General Becerra:

On behalf of the Outdoor Power Equipment Institute (OPEI) and its members, I am writing to request the confirmation of important information with respect to the implementation of the California Consumer Privacy Act (CCPA).

OPEI is an international trade association representing the manufacturers and their suppliers of non-road gasoline powered engines, personal transport & utility vehicles, golf cars and consumer and commercial outdoor power equipment ("OPE"). OPE includes lawnmowers, garden tractors, trimmers, edgers, chain saws, snow throwers, tillers, leaf blowers and other related products. OPEI member companies and their suppliers contribute approximately \$16 billion to US GDP each year. OPEI members currently distribute their products across all 50 states, through a diversity of retail outlets including independent dealers who are authorized to sell and service their equipment through a contractual arrangement.

OPEI members rely on knowing basic types of information about their customers, as allowed for under federal law, to provide them with necessary information about product recalls and warranty repairs. These core functions help our members assure that they provide their customers with the product quality and safety which they deserve and expect.

As we read the CCPA's exemption for motor vehicles, our member manufacturers of outdoor power equipment are exempt from provisions granting consumers the right to opt out product and ownership information retained or shared between a dealer and manufacturer, if the information is shared for the purpose of effectuating or in anticipation of effectuating a repair covered by a warranty or a recall.¹

Equipment manufactured by OPEI members should be treated the same as automobiles under the CCPA. The data provided by purchasers of outdoor power equipment is substantially the same as data provided by automobile consumers. As in the automotive industry, this data is critical for dealers and manufacturers to notify customers of critical updates such as warranty and recall information. We are asking you to confirm the above interpretation and to ensure regulatory parity under the CCPA between automobiles and other equipment.

Thank you for the opportunity to clarify this important matter on behalf of our members, and please notify me if we can provide any additional information or answer questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Kris Kiser", is written over a horizontal line.

Kris Kiser
President & CEO

¹ see AB-1146, California Consumer Privacy Act of 2018: Exemptions: Vehicle Information, at https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB_1146.

Message

From: Brent Smoyer [REDACTED]
Sent: 12/6/2019 6:41:38 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: PBSA Commentary on CCPA Draft Regulations
Attachments: PBSA CCPA Regulation Commentary.pdf

Attached, please find commentary from the Professional Background Screening Association (PBSA) regarding the Attorney General's draft regulations pertaining to the California Consumer Privacy Act (CCPA).

We thank you for your time and consideration.

Brent Smoyer, JD
PBSA State Government Relations &
Grassroots Director
Phone: [REDACTED]
[REDACTED]



**NAPBS is now the Professional Background Screening Association*

If you have received this communication in error, please notify us immediately by e-mail, and delete the original message.



December 6, 2019

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

RE: CALIFORNIA CONSUMER PRIVACY ACT PROPOSED REGULATIONS

On behalf of the Professional Background Screening Association (PBSA), whose members include California residents and businesses, we write to you with commentary regarding the Department of Justice's draft rules for the California Consumer Privacy Act.

As a nonprofit organization consisting of over 900 small and large companies engaged in the background screening profession, PBSA has been dedicated to providing the public with safe places to live and work since 2003. The PBSA member companies conduct millions of employment and tenancy-related background checks each year, helping employers, staffing agencies, and nonprofit organizations make more informed decisions regarding the suitability of potential employees, contractors, tenants and volunteers.

Millions of background screening reports are requested in the United States each year. Our members are hired to verify the education, employment, financial, and criminal histories of applicants. There are a number of important reasons for conducting these searches, including: (i) ensuring a safe working environment by reducing the likelihood of workplace violence; (ii) ensuring property managers have the ability to provide safe living environments for tenants, including where housing is provided for vulnerable populations; ; (iii) reducing employee theft; (iv) reducing the

110 Horizon Drive, Ste. 210, Raleigh, NC 27615, US

Phone: [REDACTED] | Fax: 919.459.2075 | Email: info@thepbsa.org

hiring of individuals based on fraudulent credentials; (v) avoiding legal exposure for negligent hiring and (vi) meeting state law requirements designed to protect vulnerable populations like the elderly, the disabled, and children.

Background screening is a “unique animal” in the data usage world and has been acknowledged as such by the California Legislature with the exemption outlined in CCPA Section 1798.145(d). Screeners are Consumer Reporting Agencies (CRA’s) and as such are highly regulated under the Federal Fair Credit Reporting Act (FCRA) by the Federal Trade Commission and Consumer Financial Protection Bureau. Additionally, our members are also regulated by a patchwork of federal, state, and local rules pertaining to data security and privacy laws including the the California Investigative Consumer Reporting Agencies Act (“ICRAA”). We follow specific privacy and safety guidelines -- both through statute and standard industry practices -- for identity theft prevention, fraud alerts, unauthorized dissemination of information, disposal of records, and other important security practices.

Further, employment-related background checks are done with full disclosure of the background check, and the express authorization and consent of the worker whose personal information is being accessed (as explicitly required by the FCRA). The current FCRA required “opt-in” ensures that policy concerns regarding a worker’s knowledge that their data is being collected are already addressed for the worker. Data that is collected, exchanged, and/or aggregated to compile the consumer report is done so with an worker’s knowledge and express permission or written instructions.

Additionally, the FCRA, a consumer protection-based statute, addresses consumer protection by placing requirements on both CRAs and end-users (employers or property managers) who request background reports on potential employees or tenants. The regulation requires disclosure and authorization before a report is prepared and provides consumers with the right to dispute the completeness or accuracy of a report. In the event of a dispute, a CRA is also required to reinvestigate at no charge to the consumer and with strict guidelines while doing so. Please see the attached enclosure describing the many consumer protections provided within the FCRA when consumer reports are prepared for employment and tenant related background screening.

We understand that our colleagues at the Consumer Data Industry Association (CDIA) have produced a very thoughtful analysis that they are submitting, highlighting key areas where the most recent draft of these draft regulations could be improved and help consumers and business alike to easily understand their rights and obligations under the CCPA. We at PBSA have serious concerns about several sections of the proposed regulations that, if finalized, would impose greater requirements and restrictions than those provided for in the CCPA. As CDIA describes in their highly detailed analysis, these sections do not implement any particular provision in the CCPA and exceed the law’s authorization for the OAG to adopt regulations “necessary to further the purposes of” the law.

PBSA shares these concerns with CDIA and fully endorses those same suggestions for improvement. As such, we will not unnecessarily revisit them here. What we would do is emphasize three critical concerns that we at PBSA feel are most notable:

1) Remove “government entities” from the definition of “categories of sources.”

Section 999.301(d) provides a definition for “*categories of sources*,” which must be disclosed in Right to Know requests and in a business’ online privacy policy. The proposed definition includes “*government entities from which public records are obtained.*”

ISSUE: The CCPA was amended by the Legislature in 2019 to remove “*publicly available*” information – which includes government records – from the definition of “personal information”. Because publicly available government records would not be included in a consumer’s Right to Know request, businesses should not be required to disclose that it has received information from government entities from which public records are obtained.

PROPOSED SOLUTION: Strike the phrase “*government entities from which public records are obtained*” from the definition of “*categories of sources*” at section 999.301(d), to match with the Legislatures CCPA amendments.

2) Clarify business’ requirement to describe consumers’ right to delete.

Section 999.308(b)(2)(a) requires businesses to explain, in their online privacy policy, that a consumer has the right to request the deletion of their personal information **maintained** by the business. Under CCPA section 1798.105(a), consumers have the right to request a business delete any personal information about the consumer which the business has collected from the consumer but is silent as to information maintained by the business. Thus, this right of deletion under the CCPA does not extend to any information **maintained** by the business (most notably, information collected from sources other than the consumer).

ISSUE: This section requires businesses to explain to consumers their right to request deletion of personal information maintained by the business, but the CCPA only provides this right for personal information that the business **collected from the consumer**. Consumers have no right under the CCPA to request deletion of personal information a business collected from a source other than the consumer. Requiring businesses to describe consumers’ right in this way would risk confusion of consumers as to their rights under the CCPA.

PROPOSED SOLUTION: Strike the words “*or maintained.*”

3) Strike the requirement that businesses treat user-enabled privacy controls as opt-out requests.

Section 999.315(c) requires that businesses treat user-enabled privacy controls that communicate or signal a consumer's choice to opt out of the sale of their personal information to third parties as a valid request to opt out for that browser or device or, if known, for the consumer. The CCPA protects "*personal information*," which is, as stated in CCPA section 1798.140(o)(1), information that reasonably may be linkable to a particular person or household, not merely a device.

ISSUE: The CCPA does not protect information that cannot reasonably be linked to a particular person or household, regardless of whether the business can detect that the information relates to a particular device. To require this exceeds the scope of the CCPA and, as such, the OAG would be exceeding its authority under the law by attempting to impose this requirement.

To the extent that information may reasonably be linked to a particular consumer or household, consumers can install browser privacy controls for a variety of reasons, many of which do not equate to desiring for their information not to be sold to third parties. The CCPA does not provide for a right to be opted out from the sale of personal information by installing any browser privacy control. Furthermore, this technology is evolving and there will likely be compatibility problems with these controls.

PROPOSED SOLUTION: Eliminate the requirement that user-enabled privacy controls be treated as opt-out requests.

4) Properly balance the timing of regulation enactment and business compliance.

Given the high level of technicality of these proposed regulations, businesses will need significant time to develop and implement processes compliant with these requirements. Due to the effort it will take for businesses to adapt with proper compliance measures, we would respectfully request that the Attorney General provide for an implementation period of at least 6 months after publication of the final rule before the regulations would become effective.

Additionally, because of the nature of certain requirements, PBSA would respectfully request that any responsibility that is contingent upon the providing of notice prior to taking certain action either be subject to a later effective date or subject to a delayed enforcement date of at 3 months after the effective date of the primary rule.

We believe that these are reasonable requests in order to allow businesses to adapt to the regulations and that adopting regulations with delayed effective and enforcement dates will fully comply with the directive given to the Attorney General under the CCPA.

While we harbor greatest concern over the previously listed points, PBSA would once again state our vigorous support of the concerns and solutions stated in the CDIA commentary as the OAG works to improve these draft regulations.

We thank you for taking the time to hear our concerns and consider our requests. PBSA and its members are prepared to discuss any questions you may have and look forward to working with you further. Please feel free to contact me directly with any questions at [REDACTED] or [REDACTED]

Sincerely,

A handwritten signature in black ink that reads "Brent Smoyer". The signature is fluid and cursive, with the first name "Brent" and last name "Smoyer" clearly legible.

Brent Smoyer, JD
PBSA State Government Relations &
Grassroots Director



Message

From: Jacob Snow [REDACTED]
Sent: 12/6/2019 8:00:09 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Privacy and Consumer Coalition Comments on Proposed CCPA Rulemaking
Attachments: Privacy and Consumer Coalition Comments on Proposed CCPA Rulemaking.pdf

Office of the Attorney General,

Please find attached comments on the proposed rulemaking under the California Consumer Privacy Act, joined by the following organizations:

Access Humboldt
ACLU of California
CALPIRG
Center for Digital Democracy
Common Sense Kids Action
Consumer Reports
Consumer Federation of America
Digital Privacy Alliance
Electronic Frontier Foundation
Media Alliance
Oakland Privacy
Privacy Rights Clearinghouse

Best,

Jake

Jake Snow
Technology and Civil Liberties Attorney
ACLU of Northern California
he/him/his | [REDACTED] | [REDACTED]

Comments to the
Office of the Attorney General of California

Notice of Proposed Rulemaking
The California Consumer Privacy Act

Submitted via Email to PrivacyRegulations@doj.ca.gov

December 6, 2019

On Behalf of the Following Organizations:



Table of Contents

Introduction	4
Signing Organizations	5
New Regulations Should Clarify That the CCPA Applies to Adtech	7
Section 999.301. Definitions	8
The draft regulations safeguard the definition of personal information.	9
301(a). Robust “affirmative authorization” will protect young people.	9
301(d) & (e). “Categories” must be understandable to consumers.	10
Section 999.305. Notice at Collection of Personal Information	11
305(a)(1–2). Clear notice-at-collection rules will aid consumer understanding. ..	11
305(a)(3). Use beyond noticed purpose should require explicit consent.	12
305(d). Notice at collection should apply to all businesses.	13
Section 999.307. Notice of Financial Incentive	14
307(b)(5). Transparency about “pay for privacy” is good for consumers.	14
Section 999.308. Privacy Policy	15
Section 999.312. Methods for Submitting Access and Deletion Requests	15
312(c). CCPA requests should be available in familiar ways.	16
312(d). A two-step deletion process will likely protect consumers.	16
312(f). Businesses should assist consumers with defective requests.	16
Section 999.313. Responding to Requests to Know and Requests to Delete	17
313(c)(1). Verification should be required to get specific information.	17
313(c)(3). An overbroad “risk to security” exception is bad for consumers.	17
313(c)(4). Certain extraordinarily sensitive information need not be disclosed. ..	18
313(c)(5) & 313(d)(6)(B). All refusals to comply should be explained.	18
313(c)(7). Self-service portals may aid consumers in exercising their rights.	19
313(d)(2)(b) & (c). Deidentification is not the same as deletion.	20
313(d)(6)(A). Deletion request refusals should be explained.	20
313(d)(7) & 315(d). The draft regulations could rein in manipulative design.	20
Section 999.314. Service Providers	21
314(a) & (b). The scope of “service provider” should be narrowly drawn.....	21

314(c). Service providers should not combine sets of personal information.	21
314(d). Service providers should explain any refusal to comply.	22
Section 999.315. Requests to Opt-Out.....	23
315(a) & (c). Browser headers are a good way to opt-out from sale.....	23
315(b). A variety of opt-out methods protects consumers.....	24
315(f). Opt-out requests should constitute an opt-out to third parties as well....	24
315(h). Opt-out requests need not be a verifiable request.....	24
Section 999.317. Training; Record-Keeping	25
317(g). More businesses should publish compliance metrics.	25
Section 999.318. Requests to Access or Delete Household Information	26
Section 999.323. General Rules Regarding Verification	26
323(a) & (d). Businesses should establish reasonable verification measures.....	26
323(c). Verification information should not be used for anything else.	26
Section 999.324. Verification for Password-Protected Accounts	27
324(a). Re-authentication can protect consumers from adversaries.....	27
Section 999.325. Verification for Non-Accountholders	28
325(a). Verification methods should be available to non-accountholders.....	28
325(c). Verification should avoid using publicly available information.....	28
325(e)(2). Businesses should adopt flexible verification procedures.....	29
325(f). Consumers should be informed when verification is not possible.....	30
Sections 999.330–332. Special Rules Regarding Minors	30
Section 999.336. Discriminatory Practices.....	30
Consolidated markets pose heightened risks.....	31
Businesses may not charge more when consumers exercise their right to know.	31
Section 999.337. Calculating the Value of Consumer Data.....	32
337(b)(5). Transparency in valuation should aid consumer understanding.....	32
337(b)(3). Varying value by group threatens to harm the most vulnerable.....	33
Conclusion.....	34

Introduction

The undersigned group of privacy and consumer-advocacy organizations thank the Office of the Attorney General for its work on the proposed California Consumer Privacy Act regulations. The draft regulations bring a measure of clarity and practical guidance to the CCPA's provisions entitling consumers to access, delete, and opt-out of the sale of their personal information. The draft regulations overall represent a step forward for consumer privacy, but some specific draft regulations are bad for consumers and should be eliminated. Others require revision. The coalition highlights the following requests from our detailed analysis below:

Ensure adtech compliance. We encourage the Attorney General to issue clarifying regulations that will plainly prohibit the plan that some members of the advertising technology industry have announced as their intended way of “complying” with the CCPA. These plans represent an attempt to deprive consumers of their right to opt-out under the CCPA, and the Attorney General should make abundantly clear—without waiting to signal what the law requires through an enforcement action—that “sale” under the CCPA includes the most pervasive and invasive form of information sale: passing information for targeted advertising.

Maintain meaningful scope of personal information. We appreciate the Attorney General's refusal—despite requests from industry to do so—to weaken the definition of personal information in the CCPA. The definition of personal information is the foundation of any privacy law, and the CCPA's definition ensures that everything that is reasonably capable of being associated with a person—not just information that identifies a person—is covered and protected.

Build on existing consumer privacy preferences. The coalition also supports the Attorney General's draft regulation directing that browser settings must be respected as an opt-out of the sale of a consumer's personal information. Many major web browsers already include settings by which users can easily choose to send “do not track” headers with all of their web traffic. And thousands of Californians have already installed tools that send “do not track” browsing headers to the sites they visit. The draft regulations should be clarified to take advantage of this existing infrastructure and respect the choices consumers have already made to protect their privacy.

Maintain strength of access right. The coalition requests that the Attorney General eliminate the overbroad exception to consumers' right to access because of a “risk to security.” This additional rule is not necessary to protect consumers from adversaries, because the draft regulations' verification requirements offer significant protection for consumers' information. The “risk to security” exception also gives businesses undue power to thwart consumer requests to know.

Limit pay for privacy. The regulations' suggestion that businesses carve up consumers by group and charge different prices according to group membership should be eliminated. People's information is most valuable not when they are rich, but when they are vulnerable. The top 100 Adwords by value, for example, are a window into the lives of people turning to the Internet for help in tragic circumstances, including keywords indicating searchers needing help with automobile accidents, water damage, addiction rehabilitation, and workers' compensation. Other research shows that African American and Latinx borrowers are charged higher interest rates and are therefore more profitable to mortgage lenders. Permitting businesses to price according to class or group membership has the potential to further harm communities already subject to discrimination.

Ensure consumers have meaningful protections from data brokers. Data brokers buy and sell consumer profiles and information in a manner that is totally opaque to consumers. Consumers almost never intend to interact with or share their information with data brokers, and can have trouble identifying data brokers, let alone understanding their business practices. The Attorney General regulations should not give special exemptions to such companies. Rather, the regulations should require that data brokers, like other CCPA businesses, notify consumers when they collect information about them. Further, any expansion of "service provider" to those who provide services to non-CCPA businesses should not include data brokers.

Signing Organizations

Access Humboldt is a non-profit, community media & broadband access organization serving the residents and local jurisdictions of Humboldt County on the North Coast of California USA, managing resources that include: cable access TV channels; KZZH FM 96.7 community radio; a wide area broadband network with dedicated optic fiber connections to twenty locations serving local jurisdictions and community anchor institutions; broadband access wireless networks; a Community Media Center with studio and other production equipment and training on the Eureka High School campus; and ongoing operational support for public, educational and governmental access media services.

The American Civil Liberties Union is a national, non-profit, non-partisan civil liberties organization with more than 1.6 million members dedicated to the principles of liberty and equality embodied in both the United States and California constitutions. The ACLU of California is composed of three state affiliates, the ACLU of Northern California, Southern California, and San Diego and Imperial Counties. The ACLU California operates a statewide Technology and Civil Liberties Project, founded in 2004, which works specifically on legal and policy issues at the

intersection of new technology and privacy, free speech, and other civil liberties and civil rights.

CALPIRG is a consumer group that stands up to powerful interests whenever they threaten our health and safety, our financial security or our right to fully participate in our democratic society. CALPIRG researchers uncover the facts and its staff bring its findings to the public, through the media as well as one-on-one interactions. CALPIRG advocates are bringing the voice of the public to the halls of power on behalf of consumers.

The Center for Digital Democracy's mission is to advance the public interest in the digital age. It is recognized as one of the leading consumer protection and privacy organizations in the United States. Since its founding in 2001 (and prior to that through its predecessor organization, the Center for Media Education), Center for Digital Democracy has been at the forefront of research, public education, and advocacy holding commercial data companies, digital marketers, and media companies accountable.

Common Sense Media, and its policy arm Common Sense Kids Action, is dedicated to helping kids and families thrive in a rapidly changing digital world. Since launching in 2003, Common Sense has helped millions of families and kids think critically and make smart choices about the media they create and consume, offering age-appropriate family media ratings and reviews that reach over 110 million users across the country, a digital citizenship curriculum for schools, and research reports that fuel discussions of how media and tech impact kids today. Common Sense also educates legislators across the country about children's unique vulnerabilities online.

The Consumer Federation of America is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

The Digital Privacy Alliance is a coalition of technologists, tech companies, startups, engineers, developers, activists, and advocates that fight for Internet privacy and safety. Digital Privacy Alliance members help policymakers at the state, federal,

and local levels learn about new and emerging technologies and advocate for laws that promote transparency and security on the Internet.

The Electronic Frontier Foundation works to ensure that technology supports freedom, justice, and innovation for all the people of the world. Founded in 1990, EFF is a non-profit organization supported by more than 30,000 members.

Media Alliance is a Bay Area democratic communications advocate. Media Alliance members include professional and citizen journalists and community-based communications professionals who work with the media. Its work is focused on an accessible, affordable and reliable flow of information to enable civic engagement, meaningful debate and a safe and aware populace. Many of Media Alliance's members work on hot-button issues and with sensitive materials, and those members' online privacy is a matter of great professional and personal concern.

Oakland Privacy is a citizen's coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment. As experts on municipal privacy reform, Oakland Privacy has written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

Privacy Rights Clearinghouse is dedicated to improving privacy for all by empowering individuals and advocating for positive change. Founded in 1992, Privacy Rights Clearinghouse has focused exclusively on consumer privacy issues and rights. Privacy Rights Clearinghouse strives to provide clarity on complex topics by publishing extensive educational materials and directly answering people's questions. It also amplifies the public's voice in work championing strong privacy protections.

New Regulations Should Clarify That the CCPA Applies to Adtech

Because adtech companies, under the auspices of the Interactive Advertising Bureau (IAB), have signaled that they plan to avoid compliance with the CCPA,¹ the Attorney General should use its authority to regulate companies' compliance with an opt-out request² and its authority to issue regulations as necessary to

¹ See Consumer and Privacy Group Comments on CCPA Compliance Framework for Publishers & Technology Companies (Nov. 6, 2019), <https://advocacy.consumerreports.org/research/consumer-and-privacy-group-comments-on-ccpa-compliance-framework-for-publishers-technology-companies/>.

² Cal. Civ. Code § 1798.185(a)(4)(B).

further the purposes of the title³ in order to ensure that adtech companies cannot take advantage of possible ambiguities in the CCPA.

The IAB framework claims to offer publishers options to circumvent that primary purpose of the CCPA,⁴ and purports to send consumers to existing failed self-regulatory mechanisms to exercise choices about targeted advertising⁵—despite the fact that the ineffectiveness of those programs was the reason for legislative intervention. The CCPA has a broad definition of sale that includes the transfer of data between unrelated companies for advertising purposes.⁶ The regulations should resolve the matter conclusively: circumvention efforts from the adtech industry do not comply with the law.

Three clarifications are necessary. First, the Attorney General should promulgate regulations reflecting that the transfer of data between unrelated companies for any commercial purpose falls under the definition of sale, so that consumers can opt-out of the sharing of their data for targeted advertising. Second, the Attorney General should clarify that only the company with which the consumer is *intending* to interact is a business collecting directly from the consumer. And third, the regulations should state that when the consumer has opted out, data cannot be shared to target advertising on another site or service, even with a service provider.

Relatedly, the Attorney General should tighten the business purpose exemption for service providers. Given that Facebook has given companies like Microsoft, Amazon, and Spotify extensive access to consumer data under the guise of a “service provider” relationship,⁷ the regulations should state that sharing in spite of an opt-out instruction must be reasonably constrained and proportionate, and subject to reasonable retention requirements.

Section 999.301. Definitions

³ Cal. Civ. Code § 1798.185(b)(2).

⁴ IAB CCPA Compliance Framework for Publishers & Technology Companies Version 1.0, Interactive Advertising Bureau (Dec. 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf (“IAB Framework”).

⁵ IAB Framework at (III)(2)(d)(ii).

⁶ Cal. Civ. Code § 1798.140(t)(1).

⁷ Gabriel J.X. Dance, Michael LaForgia and Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. Times (Dec. 18, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

The draft regulations safeguard the definition of personal information.

The Attorney General has appropriately rejected industry requests to narrow the definition of personal information in the draft rules. Some industry representatives have sought to dramatically scale back the information covered by the CCPA, particularly information associated with a device, such as IP addresses, information associated with a household, as well as pseudonymous information.⁸ These efforts were rejected by the legislature.⁹ The Attorney General should continue to reject requests to narrow information covered by the CCPA, which would eliminate important rights for consumers and directly counter legislative intent.

Limiting the definition of personal information would remove consumers' ability to opt out of its sale—a key protection under the law. Device and household-level data is very sensitive, and consumers deserve protections around its use. For example, removing IP address from the definition of personal information would weaken protections against the sale of location data to adtech companies, data brokers, and other third parties. Correlation of IP addresses is a means for companies to engage in cross-device tracking, as devices that share local networks are considerably more likely to be operated by the same persons.¹⁰

301(a). Robust “affirmative authorization” will protect young people.

The CCPA requires “affirmative authorization” before consumers under 16, or parents of consumer under 13, may opt in to the sale of their information. Sec. 1798.120(c). The Attorney General’s draft regulations offer a robust definition for affirmative authorization that includes a two-step process. The coalition strongly supports this.

This definition minimizes the possibility that a teen will accidentally or inadvertently click on or “opt-in” to something they do not truly want. This is a real risk because current site designs can manipulate users to click a button without understanding the consequences. This risk is heightened by the fact that consumers navigating these sites include time-strapped parents, teens whose brains are still developing, and individuals for whom English may not be a first language.

⁸ Letter from California Chamber of Commerce et al. to Bill Dodd, Re: SB 1121 (Dodd): Business Community Requests to be Included in AB 375 Clean-Up Legislation at 4–6 (Aug. 6, 2018), <http://src.bna.com/A44> (“Chamber Letter”).

⁹ Maria Dinzeo and Nick Cahill, *Efforts to Gut Consumer Privacy Act Largely Fail*, Courthouse News Service, July 10, 2019, available at <https://www.courthousenews.com/efforts-to-gut-consumer-privacy-act-largely-fail/>.

¹⁰ *Cross-Device Tracking: An FTC Staff Report*, Fed. Trade Comm’n at 3 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

301(d) & (e). “Categories” must be understandable to consumers.

In Section 301(d) and 301(e), the Attorney General addresses the meaning of “categories” of sources of personal information and “categories” of third parties. The coalition is concerned, however, that these definitions do not provide clarity and guidance about to how to describe those categories to consumers under the CCPA. In order to meet the goal expressed in the Attorney General’s Initial Statement of Reasons (ISOR), which is to benefit consumers by ensuring that the information is specific enough for them to understand the businesses’ data practices, businesses must use terms that consumers can demonstrably understand.

First, the Attorney General should revise the wording in Section 301(e) regarding categories of third parties. The definition of “third party” in CCPA Section 140(w) describes entities as third parties in terms of their relationships to the business that is collecting the consumer’s data. But many entities operating as third parties may collect personal information directly from consumers in other circumstances. To ensure that these companies are appropriately covered under the CCPA, the Attorney General should adopt the following definition:

“Categories of third parties” means the types of entities that ~~do not collect personal information directly from consumers~~ **are acting as third parties in relation to the business as defined by 1798.140(w) and to which the business sells consumers’ personal information as defined by 1798.140(t)(1)**, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.

Second, the Attorney General should establish a detailed and standardized system to classify the terms used in consumer notices to describe the categories of entities, types of personal data, and purposes of data use.¹¹ These terms should be independently tested with consumers to ensure comprehensibility.

The categories used in Section 301(e) were drawn primarily from the multistakeholder (MSH) process facilitated by the National Telecommunications and Information Administration (NTIA) to develop a model mobile app privacy

¹¹ The North American Industry Classification System (NAICS) could be a helpful model. NAICS is “the standard used by Federal agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy.” It aims to “provide uniformity and comparability in the presentation of statistical data describing the U.S. economy.” The Federal Trade Commission, for example, requires merging parties to include NAICS classification codes for their businesses in connection with merger filings.

<https://www.ftc.gov/enforcement/premerger-notification-program/hsr-resources/overview-naics>

policy.¹² Some members of the coalition participated in that process. These categories should not be used as a model because of problems with the MSH process and because research shows that consumers will not be able to understand them.¹³

Researchers tested the terms developed through the MSH process using an online survey of 791 individuals plus four participants in the MSH. The survey showed that the categories were not well understood. Even the MSH participants disagreed on the right categories in the scenarios they were given. Of particular relevance here, the categories for third parties fared poorly; for instance, most survey respondents understood what government entities and carriers were, but not data resellers.

The wording of key information about businesses' data practices must be tested to ensure that it is comprehensible to consumers. Consumers cannot make informed choices about whether to interact with businesses, to request information about the data that has been collected about them and what has been done with it, to opt out of their data being sold, to accept a financial incentive, or to delete their data without a clear understanding of the businesses' data practices.¹⁴

The dual purposes of transparency and control are not served by a system of classification that is overly general and non-standardized. Such a rule risks leaving businesses free to develop their own classification systems, which may not provide the necessary specificity and comprehensibility.

Section 999.305. Notice at Collection of Personal Information

305(a)(1–2). Clear notice-at-collection rules will aid consumer understanding.

The Attorney General's draft regulations implementing the CCPA's notice requirements will help consumers understand these notices, thereby making such notices more meaningful. The CCPA provides a number of new transparency rights to consumers, including notice at the point of collection about information that is collected and sold. CCPA Sec. 1798.100. The CCPA additionally requires that the Attorney General "[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

¹² NTIA, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices*, (July 25, 2013), https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

¹³ For more information about the NTIA MSH process and results, see Rebecca Balebako, Richard Shay, Lorrie Faith Cranor, *Is Your Inseam a Biometric? A Case Study on the Role of Usability Studies in Developing Public Policy*, Carnegie Mellon University (February 2014), <http://lorrie.cranor.org/pubs/usec14-inseam.pdf>.

¹⁴ The same concerns about consumer comprehension in regard to Sections 301(d) and (e) also arise in other Sections including 301(n), 305(a) and (b), 306(a), 307(b) (2), 308(a) and (b), 313, and 315(d).

the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer.” CCPA Sec. 1798.185(a)(6).

It is important that (in the words of the draft regulations) notice be “easy to read and understandable to an average consumer,” using “plain, straightforward language,” and that notices “avoid technical or legal jargon.” The coalition further supports the requirements that (a) in mobile contexts, formats should be adjusted to reflect smaller screens, (b) if a business typically conducts itself in a language other than English, those languages should also be used in notices, and (c) notices should be accessible to consumers with disabilities.

The draft regulations appropriately address “offline” collection as well. Information collection increasingly takes place in physical spaces, often in ways that are passive and hidden (such as Bluetooth beacons that track consumers’ devices or hard-to-spot cameras that record consumers’ faces). So it is critical that such collection be called out and explained to consumers. However, a notice solely providing a link to a website where information can be found is not sufficient. Rather, physical notices should highlight specific types of tracking that consumers would find relevant or important, such as audio, video, location, or biometric information collection. Companies should also be required to inform consumers if they sell information collected about consumers at the time of sale.

The coalition proposes the following revision to Section 305(a)(2)(e):

“(e) Be visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage ~~or~~ **and** the mobile application’s download page ~~or~~ **and** on all webpages where personal information is collected. When a business collects consumers’ personal information offline, it may, for example, 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 the web address where the notice can be found **and identifying any audio, video, location, or biometric information collection and whether the business sells any personal information.**”

305(a)(3). Use beyond noticed purpose should require explicit consent.

The coalition supports the Attorney General’s draft regulations requiring direct notification and explicit consent before additional uses may be made with consumers’ information. Under the CCPA, businesses can only collect and use information with notice to a consumer. A business is prohibited from further collection without providing “notice consistent with this section.” CCPA Sec. 1798.100(b).

The draft regulations operationalize the requirements in the CCPA. Simply putting up a new notice on a website after a consumer has already provided personal information, when that consumer may be unlikely to revisit the website (and is certainly unlikely to revisit the notice) is not meaningful consumer notice under the CCPA. It would leave the vast majority of consumers without knowledge when businesses change practices midstream. So the draft regulations advance the goal of the CCPA: to advance consumer privacy.

305(d). Notice at collection should apply to *all* businesses.

The draft regulations in Section 305(d) should be revised to ensure that data brokers are required to notify consumers when they collect information about them. Under the CCPA, any business that collects a consumer’s personal information must inform consumers as to “categories of personal information to be collected and the purposes for which the categories of personal information shall be used.” CCPA Sec. 1798.100(b). This statutory generalized notice-at-collection requirement applies to *all* businesses that collect personal information, not just those that collect information directly from the consumer.

On this point, the draft regulations are a step backward. Under Section 305(d), a business that does not collect information from a consumer—a data broker, for example—can collect information about a consumer without any notice. This exception undercuts the CCPA’s core transparency mandate. Instead, it would allow the data brokers and other businesses to collect information about consumers out of the public eye.¹⁵ Moreover, Section 305(d) is inconsistent with the draft regulations themselves, which state in Section 305(a)(4) that “[a] business shall not collect categories of personal information other than those disclosed in the notice at collection.” Section 305(a)(4) rightly applies to all collections of personal information by a business, whether directly from the consumer or not.

The draft regulations also permit a company that does not collect information directly from consumers to sell information about a consumer if it does one of two things: *either* contact the consumer directly, and notify them of their right to opt-out of the sale; *or* obtain confirmation from the source of the personal information that the notice-at-collection procedures were followed. But direct contact to the consumer should be the default requirement: a certification from the source fails to achieve the transparency purpose of the CCPA and should only be used if necessary.

The coalition therefore proposes the following revision to Draft Regs. Section 305(d):

¹⁵ See Frank Pasquale, *The Dark Market for Personal Data*, New York Times, October 16, 2014, available at <https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html>.

~~(d) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but b~~Before ~~it a~~ **business** can sell a consumer's personal information, it shall ~~do either of the following:~~

- (1) Contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306, **or if contacting the consumer directly is not possible;**
- (2) Contact the source of the personal information to:
 - a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and
 - b. Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer upon request.

Section 999.307. Notice of Financial Incentive

307(b)(5). Transparency about “pay for privacy” is good for consumers.

The Attorney General's draft regulations require businesses to disclose certain information about financial incentives. *See generally* Draft Regs. Sec. 307. The coalition supports these transparency requirements, as a means to mitigate some harms of the “pay for privacy” provisions of CCPA.

CCPA generally bars businesses from discriminating against consumers for exercising their CCPA rights, for example, by charging a higher price or providing a lower quality. CCPA Sec. 125(a)(1). Unfortunately, CCPA exempts from this rule certain “financial incentives.” CCPA Secs. 125(a)(2) & (b). Members of the coalition oppose this exemption because data privacy is a fundamental human right and a constitutional right in California.¹⁶ These financial incentives encourage everyone to surrender their right to privacy, and these incentives will lead to a society of income-based “privacy haves” and “privacy have nots.” The CCPA to some degree mitigates this harm by requiring the Attorney General to promulgate regulations regarding disclosure of information by businesses about such financial incentives. *See* CCPA Sec. 185(a)(6).

¹⁶ Constitution of the State of California, Article I, Section 1.
https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS§ionNum=SECTION%201.&article=I.

Among other things, the coalition in this context supports the requirement that businesses provide “an explanation of why the financial incentive or price or service difference is permitted,” including “a good-faith estimate of the value of the consumer’s data,” and “a description of the method the business used to calculate the value.” *See* Draft Regs. Sec. 307(b)(5). This rule will tend to limit the harm of “pay for privacy.” The rule will stop some businesses from over-charging and enable consumers to make informed choices.

Section 999.308. Privacy Policy

The Attorney General’s proposed guidelines for privacy policies will likely help consumers better understand their rights under the law, but companies should also be required to provide more information about how they use and process data, to help rein in business practices that violate consumer privacy. While many consumers do not read extensive privacy policies,¹⁷ many interested parties do read them, so they serve a real purpose. The FTC, for example, typically takes action against companies for privacy reasons only when they violate their terms of service.¹⁸ Because there are few requirements for these disclosures, and because most FTC privacy cases are predicated upon a specific misstatement in a privacy policy or elsewhere, many companies tend to make privacy policies as permissive as possible, so as to shield themselves from lawsuits and other enforcement actions.¹⁹ To address this problem, companies must be required to detail their practices in their privacy policies. The primary audience is not the average consumer, but instead regulators, the press, and consumer or advocacy organizations.

These documents should be used primarily as compliance and accountability tools—so that companies can be held accountable for the standards set forth in these documents. The Attorney General should set guidelines to ensure that the privacy policies accurately and thoroughly describe companies’ privacy and security practices. This will improve transparency and help rein in abusive privacy practices.

Section 999.312. Methods for Submitting Access and Deletion Requests

¹⁷ Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats* at 6, <https://www.robreeder.com/pubs/PETS2009.pdf>.

¹⁸ Protecting Consumer Privacy in an Era of Rapid Change, Fed. Trade Comm’n at 8-9 (Dec. 2010), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>.

¹⁹ *Id.* at 19.

312(c). CCPA requests should be available in familiar ways.

The coalition supports the Attorney General’s proposed methods for submitting access and deletion requests. CCPA requires businesses to provide consumers two or more methods to submit CCPA requests. *See* CCPA Sec. 130(a)(1). The Attorney General’s draft regulations provide that at least one of these methods “shall reflect the manner in which the business primarily interacts with the consumer,” e.g., “if the business is an online retailer, at least one method by which the consumer may submit requests should be through the business’s retail website.” *See* Draft Regs. Sec. 312(c). The coalition supports this rule, as a way to make it easier for consumers to make CCPA requests to businesses.

CCPA also requires certain businesses to allow consumers to make CCPA requests by means of a toll-free number and/or the businesses’ website. *See* Sec. 130(a)(1). The Attorney General’s draft regulations provide that a business must allow CCPA requests in the manner that consumers primarily interact with the business, even if this results in the business having to provide a third way for consumers to make requests (in addition to a toll-free number and the business’ website). *See* Draft Regs. Sec. 312(c). The coalition supports this rule, as an additional way to make it easier for consumers to make CCPA requests to businesses.

312(d). A two-step deletion process will likely protect consumers.

The CCPA enables consumers to request the deletion of their information. CCPA Sec. 1798.105. The coalition supports the Attorney General’s proposal that requests to delete should use a two-step process, whereby consumers submit and then confirm their deletion request. The coalition supports this requirement because it will help ensure that consumers do not accidentally delete their information. While it is not the coalition’s expectation that sites will try to push consumers to delete information, in the same way that they may push consumers to opt-in to information sales or other privacy detrimental behavior, deletion is nonetheless a permanent step and online interfaces can be confusing for consumers. Helping to ensure that consumers do not accidentally delete information is a beneficial protection. It is also helpful to businesses who can be more assured that consumers requesting deletion intend to do so.

312(f). Businesses should assist consumers with defective requests.

The coalition supports the Attorney General’s draft regulation requiring that a business support consumers when requests are deficient. That is, if a business declines to comply with a consumer’s request to access, delete, or opt-out of the sale of their personal information if the consumer did not use the correct method to make their request, or if the request is otherwise deficient, the business must either (i) comply with the request despite the deficiency, or (ii) give the consumer “specific

directions” on how to properly submit the request or to remedy the deficiency. *See* Draft Regs. Sec. 312(f). The coalition supports this rule because it will facilitate effective consumer requests.

Section 999.313. Responding to Requests to Know and Requests to Delete

313(c)(1). Verification should be required to get specific information.

The coalition supports the Attorney General’s proposal that a business shall not disclose specific pieces of personal information in the event that it cannot verify a consumer request. *See* Draft Regs. Sec. 303(c)(1). CCPA requires a business to disclose the specific pieces of personal information that the business has collected about a consumer pursuant to a verifiable consumer request. CCPA Sec. 1798.110(a)(5) & (b). It is silent on whether the business may disclose specific pieces of personal information if an otherwise-valid request is not verifiable.

In the situation where a business legitimately is unable to verify that the requester is the consumer, there is an unacceptable risk that the information will be disclosed to a third party who might have adversarial interests to the consumer. The regulations properly avoid that outcome by allowing disclosure under a request to know only if the request is in fact verified.

313(c)(3). An overbroad “risk to security” exception is bad for consumers.

The coalition opposes the Attorney General’s proposal to prohibit companies from disclosing specific pieces of information if disclosure would create “a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s account with the business, or the security of the business’s systems or networks.” This rule is not necessary to protect consumers from adversaries, and it gives businesses undue power to thwart consumer requests to know.

As discussed below, the CCPA properly contains various rules on verification of consumer requests; the CCPA properly requires the Attorney General to promulgate further rules on verification; and the Attorney General has promulgated various draft rules on verification. As further discussed below, many of the Attorney General’s proposed verification rules are very helpful, and some could benefit from adjustments. These verification rules are sufficient to protect the security of consumers’ personal information and accounts. So this additional Rule 313(c)(3) gives businesses unnecessary power to deny access requests for specific pieces of personal information.

The draft regulation is also unnecessary to protect “the security of the businesses’ systems or networks.” The coalition does not agree with the premise that the disclosure to a consumer of their specific pieces of personal information will ever

create risk to the security of a business' systems. It is true that some businesses secure their systems by monitoring visits, gathering information from visitors, and analyzing that information, in order to identify which visitors are adversaries that pose heightened security risks. But sophisticated adversaries can readily ascertain what information is being gathered from them when they visit systems. These adversaries might not be able to ascertain the methods businesses use to analyze that information, but such methods are likely outside CCPA's access rights. Thus, disclosure to an adversary of the specific pieces of personal information that the business gathered from the adversary will not improve the adversary's ability to intrude on the business' systems.

Moreover, many businesses take a troublingly broad view of their need for secrecy as a means to secure their systems. Many of these businesses will claim shelter within the rule's nebulous standard—"a substantial, articulable, and unreasonable risk." Because of the CCPA's unfortunate concentration of exclusive enforcement power in the Office of the Attorney General, and empowerment of businesses to evade enforcement with a 30-day cure period, it is likely that many businesses will assert overbroad interpretations of this vague and unnecessary rule.

The coalition proposes deleting Section 313(c)(3).

313(c)(4). Certain extraordinarily sensitive information need not be disclosed.

The Attorney General's draft regulations appropriately bar a business, when responding to a CCPA access request, from disclosing a small number of enumerated kinds of extraordinarily sensitive information: government-issued identification numbers (including social security numbers and driver's license numbers); financial and medical account numbers; and security passwords and questions-and-answers. *See* Draft Regs. Sec. 314(c)(4). The coalition supports this rule, because this narrow set of information is especially damaging when wrongfully disclosed, and unlikely to be sought by most consumers.

313(c)(5) & 313(d)(6)(B). All refusals to comply should be explained.

When a business refuses to comply with a request to know or delete, the draft regulations correctly provide that the business inform the consumer and explain the basis for the denial. Draft Regs. Secs. 313(c)(5), 313(d)(6). The coalition supports this rule because it gives consumers the information they need to submit an alternate request or report to the Attorney General that an exception is being claimed by a business without foundation.

The coalition also supports the requirement that a business disclose (or delete) any information that is not covered by the exception. Withholding records only in part is standard practice in public-records law and discovery practice in litigation when a

privilege applies. The same rule should apply when consumers request access to (or deletion of) their personal information.

The coalition respectfully requests that the clause “because of a conflict with federal or state law, or an exception to the CCPA” be struck, so that the regulations require a response informing the requester of the reasoning behind any denied right to know request. As written, the regulations would not require any response if the company determined that it had no records responsive to the request or was otherwise not obligated to provide the requested information, leaving the consumer uncertain as to whether the request was in fact received and processed at all.

Relatedly, the coalition supports the Attorney General’s decision not to establish an exception to consumers’ rights of access, deletion, or opt-out on the basis of trade secrets or other intellectual property rights. No such exception is necessary or appropriate. Overbroad claims of a trade-secrets privilege have, for example, been used to undermine people’s rights in other contexts,²⁰ and such abuses should not stand in the way of consumers exercising their privacy rights.

The coalition proposes the following revision to Section 313(c)(5):

(5) If a business denies a consumer’s verified request to know specific pieces of personal information, in whole or in part, ~~because of a conflict with federal or state law, or because of an exception to the CCPA~~, the business shall inform the requestor and explain the basis for the denial. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

313(c)(7). Self-service portals may aid consumers in exercising their rights.

The coalition supports the Attorney General’s proposal that businesses may use secure self-service portals to respond to access requests. CCPA requires that businesses provide consumers two or more methods to submit CCPA requests. *See* CCPA Sec. 130(a)(1). The Attorney General’s draft regulations provide that one of these methods can be “a secure self-service portal” that consumers can use “to access, view, and receive a portable copy of their personal information,” provided that: (i) the consumer has a password-protected account with the business, (ii) the portal fully discloses the data the consumer is entitled to, (iii) it uses reasonable data security controls, and (iv) it complies with verification requirements. *See* Draft Regs. Sec. 313(c)(7). The coalition supports this rule, as a way to make it easier for consumers to make CCPA requests to businesses.

²⁰ *See generally*, Rebecca Wexler, *Life, Liberty, and Trade Secrets*, 70 STAN. L. REV. 1343 (2018).

313(d)(2)(b) & (c). Deidentification is not the same as deletion.

The coalition opposes the Attorney General’s draft rule allowing companies to comply with a deletion request by deidentifying or aggregating the information. The CCPA gives consumers the right to request deletion of their information. CCPA Sec. 1798.105. There are a number of listed exceptions for when businesses do not need to comply with requests to delete information, but if an exception does not apply companies are to delete the information requested. CCPA Sec. 1798.105(d). The draft regulations differ from the requirements of the CCPA by enabling—in response to a consumer’s request to delete—the companies to instead deidentify or aggregate the consumer’s personal information. Deidentifying and/or aggregating information is not the same as deleting it. Businesses should do what consumers request unless an exception applies.

While deidentified and aggregate information are outside of the scope of “personal information” under the CCPA, companies should be incentivized to maintain information as deidentified or aggregate as a general matter of course, not wait until they receive a request to delete to do so. Treating a request for deletion as a request to deidentify or aggregate will only encourage companies to wait until such a request is made before they take privacy protective steps.

The coalition proposes deleting subsections 313(d)(2)(b) & (c).

313(d)(6)(A). Deletion request refusals should be explained.

The coalition supports the Attorney General’s proposal to require companies to explain any denials of consumer requests to delete their data. CCPA empowers consumers to ask businesses to delete their personal information, subject to various exemptions. *See* CCPA Sec. 105. The Attorney General draft regulations provide that if a business denies a deletion request, it shall notify the consumer of the denial, and “describe the basis for the denial, including any statutory and regulatory exception therefor.” Draft Regs. Sec. 313(d)(6)(A). The coalition supports this rule, as a check on businesses’ power to deny deletion requests. First, with knowledge of the defect in their initial request, a consumer may be able file a correct request. Second, if the consumer does not agree with the business’ basis for denial, then the consumer can ask the Attorney General to investigate the matter.

313(d)(7) & 315(d). The draft regulations could rein in manipulative design.

The Attorney General should finalize the rules as proposed in 313(d)(7) & 315(d), which seek to rein in companies that might otherwise steer consumers to partially delete or stop the sale of their information. The rules properly require that companies must make the universal option—to delete or stop the sale of all of their information—more prominent than the option on their websites of partial deletion or sale opt-out. This guidance appropriately restrains companies that might

otherwise seek to steer consumers to the partial option through eye-catching (but deceptive) user experience design choices known as “dark patterns.”²¹ Use of dark patterns to push consumers to share more information than they would like is all too common, and the proposed rules will help prevent these practices.

Section 999.314. Service Providers

314(a) & (b). The scope of “service provider” should be narrowly drawn.

The Attorney General should clarify that service providers to non-businesses should only qualify as “service providers” in specific circumstances. The CCPA applies to businesses that meet certain thresholds, as well as other entities that interact with such businesses like service providers. CCPA Sec. 1798.140(c). Under the CCPA, a service provider is defined as an entity “that processes information on behalf of a business” following a certain set of rules and restrictions. CCPA Sec. 1798.140(v). This raises a question about companies who act as services providers in every respect except that they are processing information on behalf of a non-business, such as a government entity or nonprofit. The draft regulations would broaden this definition by enabling entities that act as service providers to non-businesses to qualify. The draft regulations also extend the definition of service provider to include those that collect information directly from consumers on behalf of a business.

While the coalition agrees that in certain contexts, such as service providers to schools, certain allowances may be helpful and appropriate, the coalition is concerned about the boundless expansion of the definition of service provider.

In particular, the coalition is concerned that major data brokers, such as Lexis-Nexis or Experian, may be able to claim that they are “service providers” to the federal or state government, and claim they collect information from broad swathes of consumers at the direction of the government, and will then be absolved of compliance with the CCPA. This is to the detriment of consumer privacy and at odds with the goals of the CCPA. Service providers to non-businesses should only qualify as “service providers” in specific, enumerated circumstances.

314(c). Service providers should not combine sets of personal information.

Section 314(c) of the draft regulations prohibit the use of information collected by a service provider for the purpose of providing a service to another person or entity. The coalition supports this rule.

²¹ Natasha Lomas, *WTF is dark pattern design*, TechCrunch (July 1, 2018), <https://techcrunch.com/2018/07/01/wtf-is-dark-pattern-design/>.

Under the CCPA, sharing a consumer’s personal information with a service provider, even in the context of a commercial relationship, does not constitute a sale of information so long the other restrictions in the statute are satisfied. *See, e.g.*, CCPA Secs. 140(v), 140(d). Among those restrictions are the requirement that a service provider be prohibited by contract from “retaining, using, or disclosing the personal information for *any purpose* other than providing the services specified in the contract.” CCPA Sec. 140(v) (emphasis added). The first sentence of Section 314(c) operationalizes the CCPA’s restriction and provides helpful clarification on what purposes are off limits for service providers.

The coalition opposes the second sentence of Section 314(c) of the draft regulations, however. That sentence would allow service providers to combine information received from multiple serviced entities and build profiles of individuals based on a general claim that the collection of information, combination across entities, and use of that information would “protect against fraudulent or illegal activity.” In the eyes of many businesses, the remote possibility of hypothetical illegal activity may justify effectively unlimited dragnet collection of all information about a person’s use of an electronic service. So, for example, every message sent between users could be captured, stored, combined, and analyzed on the off chance a message might contain some indication of an unlawful act. And every user interaction of a user could be monitored and catalogued across service-provider customers, justified by the remote possibility that the user might, in those interactions, be violating the terms of service of the app or website. The exception for fraudulent or illegal activity therefore threatens to swallow the rule.

The coalition recommends the following revision to Section 314(c) of the draft regulations, eliminating the overly broad exception:

A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity. ~~A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.~~

314(d). Service providers should explain any refusal to comply.

The Attorney General should finalize the proposed rule clarifying that if a business’s service provider denies a consumer’s request to access or delete their personal information, the service provider must (a) explain why it denied the request, (b) direct the consumer to submit to the request to the business, and (c) if possible, provide the business’s contact information. Without these requirements,

the consumer would have no way of knowing how to properly submit the request and exercise their rights under the law.

Section 999.315. Requests to Opt-Out

315(a) & (c). Browser headers are a good way to opt-out from sale.

The coalition supports the proposed rules regarding opt-outs from data sales by means of browser plugins, but requests further clarification that “Do Not Track” headings constitute a valid request to opt-out. CCPA empowers consumers to opt-out of the sale of their personal information. See CCPA Sec. 120. CCPA provides that businesses must facilitate such opt-outs by providing a “do not sell” link on their websites. *See* CCPA Sec. 135(a)(1). The Attorney General’s draft regulations identify additional means that a business may use to facilitate opt-outs, including a toll-free phone number, a designated email address, and in-person or mail-in forms. *See* Draft Regs. Sec. 315(a).

Moreover, the draft regulations require a business that collects consumer data online to treat the following as an opt-out: “user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.” Draft Regs. Sec. 315(c). A business that does not collect consumer data online may choose whether or not to treat such browser plugins and the like as an opt-out. Draft Regs. Sec. 315(a).²²

The coalition supports these proposed rules regarding opt-outs from data sales by means of browser plugins and the like, because they make it easier for consumers to exercise this important CCPA privacy right. The average California consumer interacts with a vast number of online businesses. For many consumers, it will be far easier on one occasion to install a browser plugin that opts-out of data sales by all online companies they come into contact with, compared to individual opt-out requests from the consumer to each of these many businesses.

To ensure the effectiveness of these proposed rules, the coalition requests the addition of the following sentence to the end of both Section 315(a) and 315(c):

A business shall treat a “do not track” browsing header as such a choice.

Thousands of Californians have already installed tools that send “do not track” browsing headers to the sites they visit. Many major web browsers already include

²² In proposing this, the Attorney General is exercising its authority to regulate consumers’ submission of, and business’ compliance with, opt-out requests (Cal. Civ. Code § 1798.185(a)(4)(A)-(B) and its authority to issue regulations to further the purposes of the title under Cal. Civ. Code § 1798.185(b)(2).

settings by which users can easily choose to send “do not track” headers with all of their web traffic. A business that cannot collect a person’s information cannot sell that information. The greater (do not collect) includes the lesser (do not sell). To avoid crabbed arguments from businesses that the current proposed regulations provide no relief from data sales to the thousands of Californians who have installed tools that send “do not track” browsing headers, the coalition requests this additional clarifying sentence.

315(b). A variety of opt-out methods protects consumers.

The coalition supports the Attorney General’s proposed rule that at least one opt-out method offered by each business must reflect the manner that it primarily interacts with the consumer. *See* Draft Regs. Sec. 315(b). The coalition supports this proposal because it makes it easier for consumers to exercise this important CCPA privacy right.

315(f). Opt-out requests should constitute an opt-out to third parties as well.

The coalition supports the draft regulations’ requirement in Section 315(f) that businesses notify third parties that a consumer has opted out of the sale of their personal information. That requirement should be strengthened to have the clear effect of informing third parties of the consumer’s request to opt-out, which the third parties must honor as the CCPA requires and deliver that request on to other third parties to whom personal information has been sold.

The coalition therefore proposes the following amendment to make clear that the notice to third parties that the consumer has opted out constitutes, to those third parties, an opt-out request from the consumer. The following amendment also makes two proposed changes to correct an apparent typo (“prior to”) and clarify the current meaning (“the third parties”):

(f) A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days ~~prior to~~ of the business’s receipt of the consumer’s request that the consumer has exercised their right to opt-out and instruct ~~them-the third parties~~ not to further sell the information. **The notice to third parties not to further sell the information shall constitute a request to opt-out from the consumer.** The business shall notify the consumer when this has been completed.

315(h). Opt-out requests need not be a verifiable request.

The Attorney General’s draft regulations provide in Section 315(h) that a request to opt-out need not be a verifiable request. The coalition supports this rule.

Massive volumes of personal information are collected by businesses through the ordinary operation of electronic devices and Internet services and then used to track

people, build profiles of their characteristics and behavior, and sell that information to other businesses.²³ Finally, there is little risk that a consumer's adversary might attempt to fraudulently opt-out the consumer from the sale of their personal information, and if an adversary should succeed in doing so, there would be at most de minimus injury to the consumer. For these reasons, consumers' privacy is best protected when requests to opt-out need not be verifiable.

Section 999.317. Training; Record-Keeping

317(g). More businesses should publish compliance metrics.

The Attorney General should lower the threshold for businesses required to publish metrics on their compliance with CCPA requests to those with either \$25 million in annual revenue, or 50% of revenue generated from the sale of personal information.

The coalition supports the Attorney General's proposal to require certain businesses to provide metrics on the number of consumer requests they have received under the CCPA, their response, and the median number of days spent responding to these requests—all of which must be included in their privacy policies (or make the information accessible through their privacy policy). The proposed rule also requires these companies to establish a training program for employees in responding to these requests. These rules will help ensure that these companies respond appropriately to consumer requests.

However, the proposed threshold (businesses with personal information from 4,000,000 consumers) is too high. While some small businesses arguably should not have the additional duties proposed by this rule, this threshold would exempt many mid-size businesses that should meet these duties.

The coalition proposes the following revision to Section 317(g):

(g) A business that alone or in combination, ~~annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers~~ **has annual gross revenues in excess of twenty-five million dollars or derives 50 percent or more of its annual revenues from selling consumers' personal information**, shall:

Under this proposed size threshold, if a business processes the personal information of 50,000 consumers, but does not earn \$25 million in annual revenue and/or 50% of their revenue from sale of personal information, then that business would be

²³ See generally, Data Brokers: A Call for Transparency, Federal Trade Commission Staff Report, Federal Trade Comm'n, at 13, 19 (discussing data brokers' sources and the development of profiling products, respectively) (May 2014).

exempt from this rule's mandatory publication of metrics, even though it would be covered by CCPA.

Section 999.318. Requests to Access or Delete Household Information

The CCPA offers privacy protections to information connected with a household. CCPA Sec. 1798.140(o)(1). The draft regulations reference "aggregate household information" without providing a definition. We propose that if the regulations address household information, this phrase should be defined to ensure it is understood to not include information that someone could identify with an individual.

The coalition proposes adding a definition of "aggregate household information" to Section 301 as follows:

"Aggregate household information" means information that relates to a group of consumers that constitute a household, but which is not linked or reasonably linkable to any consumer, including via a device."

Section 999.323. General Rules Regarding Verification

323(a) & (d). Businesses should establish reasonable verification measures.

The coalition supports the Attorney General's draft rules requiring companies to establish reasonable methods of verifying a consumer's identity. CCPA provides that requests to know and to delete must be "verifiable." CCPA Secs. 100(d), 105(c), 110(b), 115(b). CCPA defines a "verifiable" request, in part, as one "that the business can reasonably verify." CCPA Sec. 100(y). CCPA requires the Attorney General to issue regulations on verification, with the goals of "minimizing the administrative burden on consumers" while taking into account (among other things) "security concerns." CCPA Sec. 185(a)(7). CCPA provides that these regulations shall distinguish between requests submitted through an existing password-protected account and other requests. *Id.*

The Attorney General's proposed regulations require a business to "establish, document, and comply with a reasonable method for verifying" that the requester is the consumer. Draft Regs. Sec. 323(a). The proposed regulations also require a business to "implement reasonable security measures" to prevent fraudulent access and deletion. Draft Regs. Sec. 323(d). The coalition supports these rules, which require companies to establish reasonable verification methods.

323(c). Verification information should not be used for anything else.

The Attorney General's proposed regulations appropriately bar a business from collecting new personal information from a consumer for purposes of verification, unless "the business cannot verify the identify the consumer from the information

already maintained by the business.” *See* Draft Regs. Sec. 323(c). The proposed regulations also properly provide that if a business collects new personal information from a consumer for purposes of verification, the information “shall only be used” for verification, and the business shall delete it “as soon as practical after processing the consumer’s request.” *Id.*

The coalition supports these proposed regulations. They minimize the collection, use, and retention of personal information. Consumers should be able to exercise their rights to access and delete information without submitting to even more processing of their personal information. This includes any information submitted or collected as part of a re-login process, if one is required in order to make a request.

Section 999.324. Verification for Password-Protected Accounts

324(a). Re-authentication can protect consumers from adversaries.

The coalition supports the Attorney General’s proposed rule that consumers must reauthenticate their identity when submitting requests through a password-protected account. When CCPA requires the Attorney General to promulgate regulations about verification of consumer requests to access or delete data, CCPA distinguishes between requests submitted through an existing password-protected account, and other requests. CCPA Sec. 185(a)(7). CCPA provides that the Attorney General shall treat the former as verifiable, while the consumer is logged into the account. *Id.* As to the latter, CCPA provides that the Attorney General shall provide an authentication mechanism. *Id.* In promulgating these regulations, CCPA requires the attorney general to take into account both “the administrative burden on consumers” and “security concerns.” *Id.*

The Attorney General’s proposed regulations provide that when a business verifies a request through a consumer’s existing password-protected account, the business shall “require a consumer to re-authenticate themselves.” Draft Regs. Sec. 324(a). The coalition supports this rule. It protects the consumer from fraudulent access or deletion by an adversary who does not know the consumer’s log-in credentials, but nonetheless has control of the consumer’s logged-in account. This can happen, for example, if an adversary steals the consumer’s laptop while it is unlocked and logged into an account. Likewise, it can happen if a consumer opens their account on a shared computer at a public library, and leaves the library without logging out, after which an adversary can sit down at that computer and control the account. Requiring the requester to log out and log back in will protect the consumer from such adversaries, without imposing a significant administrative burden on the consumer. We believe that businesses should make this re log-in process as

streamlined as possible for consumers, and not as an opportunity to manipulate consumers with “dark patterns.”

Section 999.325. Verification for Non-Accountholders

325(a). Verification methods should be available to non-accountholders.

The draft regulations correctly provide for means of verification for consumers who “do not have or cannot access a password-protected account.” Draft Regs. Sec. 325(a). The coalition is supportive of the inclusion of means of verification for consumers who “cannot access” an account. This can happen, for example, if consumers initially signed up with an email address that they no longer have access to. This is not uncommon for recent graduates of educational institutions.

325(c). Verification should avoid using publicly available information.

The Attorney General should strengthen the verification requirements to better ensure that adversaries cannot easily access consumers’ accounts using publicly available information. Again, the CCPA requires the Attorney General to promulgate regulations providing an authentication mechanism when a consumer does not have a password-protected account with a business, mindful of both “administrative burden on consumers” and “security concerns.” *See* CCPA Sec. 185(a)(7).

The Attorney General’s proposed regulations provide that when a consumer requests to know specific pieces of data but does not have a password-protected account, the business shall verify “to a reasonably high degree of certainty.” Draft Regs. Sec. 325(c). This is appropriately higher than the certainty needed when requesting categories of information. *See* Draft Regs. Sec. 325(b). The proposed regulations further provide that this standard may be met by the combination of: (a) a match of at least three pieces of data provided by the requester, to data the businesses maintains about the consumer and which the business “has determined to be reliable for the purpose of verifying”; and (b) a sworn declaration that the requester is the consumer. *Id.*

The coalition proposes the following revision to Section 325(c):

(c) A business’s compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request.

Businesses shall maintain all signed declarations as part of their record-keeping obligations. **When a business determines what personal information is reliable for the purpose of verifying the consumer, the business shall make reasonable efforts to use personal information about the consumer that is not easy for the public to discover.**

It may be easy for an adversary to ascertain significant amounts of personal information about the consumer they target for fraud, such as their name, address, date of birth, even city of birth and mother's last name before it was changed. Verification that relies on such easy-to-find personal information would not be robust. When a business determines the reliability for verification of different kinds of personal information, the business should take this into account.

325(e)(2). Businesses should adopt flexible verification procedures.

Some businesses process personal information without knowing the name of the actual person associated with that information. For example, a business might associate data not with a person's name, but with a communications address, a device identifier, or an online tracking tool.

The Attorney General's draft regulations state that when a business maintains data in a manner not associated with a named actual person, the business may verify by requiring the consumer to show they are the sole consumer associated with the data. *See* Draft Regs. Sec. 325(e)(2).

The coalition has two proposed revisions to Section 325(e)(2). First, when a requester is able to show that all consumers associated with a set of data join the request, the business should not decline the request. And second, when information is associated with a communications address, that address offers a convenient and secure way to verify that the requester is the consumer.

Therefore, the coalition proposes the following revisions to Section 325(e)(2):

(2) If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer **either (i) to demonstrate that they are the sole consumer associated with the non-name identifying information; or (ii) to show that all consumers associated with the non-name identifying information consent to the disclosure or deletion. If a business maintains personal information in a manner associated with a communications address, such as a phone number or email address, and not associated with a named actual person, the business may verify the request by sending a confirmation link to that address, and asking the recipient to use that link to confirm the request.**

325(f). Consumers should be informed when verification is not possible.

The Attorney General’s proposed regulations correctly provide that “if there is no reasonable method” to verify a requester, the business shall “so state in response to any request,” and “explain why it has no reasonable method.” *See* Draft Regs. Sec. 325(f). The coalition supports this rule, which would advance transparency about the verification process. This may lead some requesters to improve the quality of the authenticating information they submit. And it will help ensure that businesses have good reasons for their verification decisions.

Sections 999.330–332. Special Rules Regarding Minors

The coalition supports the Attorney General’s proposals to implement the stronger CCPA protections with respect to minors. CCPA offers special protections for minors under 16; specifically, that businesses shall not sell such consumers’ information without affirmative authorization. For children under 13, parents or guardians must provide this authorization. CCPA Sec. 1798.120(c)–(d). Businesses must comply if they have “actual knowledge” of a consumer’s age, which under the CCPA includes businesses “who willfully disregard a consumer’s age.” CCPA Sec. 1798.120(c).

The Attorney General’s draft regulations clarify ambiguity about what ages are covered, consistent with the legislature’s 2019 amendments (children who are 16 years of age are unfortunately not covered). The draft regulations acknowledge that the CCPA gives minor consumers and their parents a say over the sale of minors’ information from offline companies as well as companies that did not collect it directly from the minor. The regulations operationalize these additional protections for youth, by giving scope to how minors and parents can provide “affirmative authorization” and how a company can identify whether it is dealing with a parent or guardian.

The coalition is supportive of the draft regulations, which include robust mechanisms for opt-in and ensure minors and parents and guardians have notice about the ability to opt-out in the future. Furthermore, the draft regulations propose COPPA-consistent mechanisms for parental consent that many businesses are already familiar with and that offer flexibility to businesses.

Section 999.336. Discriminatory Practices

The Attorney General should exercise its authority to put reasonable limits on financial incentives programs in consolidated markets and not extend financial incentives past what the statute allows.

The CCPA allows companies to offer financial incentives for the collection, sale, or deletion, of personal information to third parties. CCPA Sec. 125(b)(1). This

language was added to the CCPA over objections from consumer and privacy advocates.²⁴ Under some interpretations of this language, consumers could be forced to choose between affordable necessities and their own fundamental privacy rights, and so retailers can continue to profit off of business models that exploit consumers' privacy without meaningful consumer choice. Despite these problems, some safeguards have been put in place including that such financial incentive programs cannot be "unjust, unreasonable, coercive, or usurious." *See* CCPA Sec. 125(b)(4). The CCPA expressly authorizes the Attorney General to establish rules regarding financial incentive programs. CCPA Sec. 185(a)(6). The current draft regulations do not adequately protect consumers.

Consolidated markets pose heightened risks.

The AG should exercise this rulemaking authority and determine that financial incentive programs are prohibited (because they are unjust, unreasonable, coercive, and usurious) where markets are consolidated and consumers lack choices. Wireline Internet Service Providers (ISPs), for example, should not be allowed to charge consumers for exercising their privacy rights, because many customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged about \$30 per month or not leveraging U-Verse data for ad targeting.²⁵ Similarly, if a grocery store is the only one in town, it should be constrained in its ability to charge consumers more if they decline to participate in the collection or sale of their information. Where consumers have few choices, market forces don't impose sufficient constraints on companies seeking to penalize consumers for exercising their privacy rights. And, there is rising concentration across many industries in the United States,²⁶ further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.²⁷

Businesses may not charge more when consumers exercise their right to know.

The CCPA only permits financial incentives "for the collection of personal information, the sale of personal information, or the deletion of personal information." CCPA Sec. 125(b)(1). The CCPA does not permit a business to offer

²⁴ Consumers Union Letter re: AB 375 (Jun. 28, 2018), <https://advocacy.consumerreports.org/wp-content/uploads/2018/06/CU-Letter-AB-375-final-1.pdf>.

²⁵ 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/>.

²⁶ 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>.

²⁷ 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>.

financial incentives, for, say, the right to access information, or the right to see a privacy policy. Unfortunately, the draft regulations appear to enable companies to charge more for individuals exercising a right to know. The coalition opposes any extension of financial incentives, and proposes the Attorney General make the following changes to Section 326:

(a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right **with respect to the collection, deletion, or sale of their personal information conferred by the CCPA or these regulations**.

...

(c) Illustrative examples follow:

(1) Example 1: A music streaming business offers a free service and a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the \$5 per month payment is reasonably related to the value of the consumer's data to the business.

(2) Example 2: A retail store offers discounted prices to consumers who sign up to be on their mailing list. If the consumer on the mailing list can continue to receive discounted prices even after they have made a **request to know**, request to delete, and/or request to opt-out, the differing price level is not discriminatory.

(d) A business's denial of a consumer's **request to know**, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.

...

Section 999.337. Calculating the Value of Consumer Data

337(b)(5). Transparency in valuation should aid consumer understanding.

The coalition supports the Attorney General's proposals to improve transparency in business's valuation of consumer data. Under the CCPA, businesses are permitted to offer financial incentives so long as they are reasonably related to the value of the consumers data. Sec. 1798.125. Businesses are prohibited from offering "financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature" Sec. 1798.125(b)(4). The Attorney General is required to establish rules and guidelines governing these offerings. Sec. 1798.185(6). The draft regulations establish that businesses must offer "good-faith estimates" of consumers' data as well as describe the methods used to calculate value. This transparency is critical to

enable consumers to determine whether they wish to take an offering and regulators to determine whether an offering is fair. The coalition supports this transparency.

337(b)(3). Varying value by group threatens to harm the most vulnerable.

Section 337(b)(3) of the draft regulations directs that a business, when calculating the value of a consumer's data for purposes of offering a financial incentive, may use levels of revenue or profit from different "tiers, categories, or classes of consumers" whose data "provides differing value." The coalition opposes this authorization because it threatens to hurt the most vulnerable consumers.

Permitting different valuations for different people might seem like an innocuous application of the simple economic principle of price discrimination, i.e., charging some people more based on their willingness or ability to pay. But the implications of charging some groups more because of the value of their information compared with other groups has the possibility of deepening the harm associated with a regime that permits charging people for exercising their privacy rights.

People's information is most valuable not when they are rich, but when they are vulnerable. The top 100 Adwords by value, for example, are a window into the lives of people turning to the Internet for help in tragic circumstances.²⁸ The most valuable keyword is "best mesothelioma lawyer" (to assist with asbestos injury), followed by keywords indicating searchers needing help with automobile accidents, water damage, addiction rehabilitation, and workers' compensation.²⁹ In another ranking of keyword categories by value, the top 20 likewise included "insurance," "loans," "degree," "treatment," "credit," and "rehab."

Moreover, authorization to divide consumers by group could have discriminatory effects. In recent academic work from the Haas School of Business at UC Berkeley, researchers found that lenders charge higher interest rates to African American and Latinx borrowers, and thereby earn 11 to 17 percent more profits on those loans.³⁰ So the pricing of privacy rights based on the profits from particular groups would create new barriers to equal opportunity.

Thus, the coalition recommends that the Attorney General eliminate section 337(b)(3). For the same reasons, we also recommend that the Attorney General

²⁸ Chris Lake, *The most expensive 100 Google Adwords keywords in the US*, Search Engine Watch, <https://www.searchenginewatch.com/2016/05/31/the-most-expensive-100-google-adwords-keywords-in-the-us/>.

²⁹ *Id.*

³⁰ Laura Counts, Berkeley Haas Newsroom, *Minority homebuyers face widespread statistical lending discrimination, study finds*, <https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/>.

include a requirement that any business taking advantage of CCPA Sections 125(a)(2) or 125(b) must charge every consumer the same amount, rather than dividing consumers into groups based on value.

The coalition proposes the following additional sub-section to Section 336:

Any price or service difference offered by a business under section 999.337 shall be offered equally to all consumers.

Conclusion

The coalition appreciates the Attorney General's work on these proposed rules and urges the Attorney General to take the steps recommended in these comments to ensure that consumers' privacy rights are protected.

Message

From: Carol Stiles [REDACTED]
Sent: 12/6/2019 4:57:29 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Privacy Regulations

Regarding this subject, I thought when I selected 'No' to Facebook requests to have advertisers use my information that I didn't have to worry about Spam or annoying advertising or annoying telemarketing phone calls. I was wrong. I dug in a little deeper and found Numerous Advertisers that Facebook was STILL selling my e-mail, phone number and information to! They were tracking things I looked up and sending me annoying advertisements about them. When I said 'No' to advertisements, Facebook blatantly disregarded that and continued tracking and selling my info to outside companies. We are all sick of being bombarded by ads, telemarketing phone calls and e-mails. And I am especially disgusted that Facebook will post obvious lies about political candidates. They need to be held to higher standards.
Carol Stiles

Sent from my iPhone

Message

From: Ferber, Scott [REDACTED]
Sent: 12/6/2019 7:20:05 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Farber, David [REDACTED]
Subject: Proposed California Consumer Privacy Act Regulations
Attachments: ACP-ltr-12-6-19.pdf; ACP-ltr-3-8-19.pdf

On behalf of the Association of Claims Professionals (ACP), we respectfully submit the attached comments to the proposed CCPA regulations. While ACP members are strong proponents of individual privacy rights, they remain concerned that the unintended application of the CCPA and proposed regulations, as currently drafted, will sow confusion and discord among California consumers and result in conflicting regulatory standards for its members and the larger California business community writ large. Through the attached, the ACP writes to suggest ways of improving the text of the proposed regulations to provide consistency and clarity to CCPA application and to avoid consumer confusion over potential conflict with other California laws. This supplements and incorporates the ACP's preliminary rulemaking submission from March 8, 2019 (attached for ease of reference).

Very truly yours,
Scott Ferber


Partner

T: [REDACTED] | M: [REDACTED] | E: [REDACTED] | www.kslaw.com

[BIO](#) | [vCARD](#)

King & Spalding LLP
1700 Pennsylvania Avenue, NW
Suite 200
Washington, D.C. 20006

KING & SPALDING

King & Spalding Confidentiality Notice:

This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.



December 6, 2019

BY EMAIL

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

RE: Proposed California Consumer Privacy Act Regulations

Ladies and Gentlemen:

The Association of Claims Professionals (ACP) is pleased to respond to requests for comment on the proposed California Consumer Privacy Act (CCPA) regulations and writes to suggest ways of improving the text of the proposed regulations to provide consistency and clarity to CCPA application and to avoid consumer confusion over potential conflict with other California laws. While ACP members are strong proponents of individual privacy rights, we remain concerned that the unintended application of the CCPA and proposed regulations, as currently drafted, will sow confusion and discord among California consumers and result in conflicting regulatory standards for our members and the larger California business community writ large. We therefore submit this letter outlining suggested refinements to the proposed regulations. This supplements and incorporates our preliminary rulemaking submission from March 8, 2019 (attached for ease of reference).

ACP's Interest in the Regulations

ACP (formerly known as the American Association of Independent Claims Professionals or AAICP) was formed in 2002 as the only national association representing the interests of the nation's independent claims professionals. ACP members employ thousands of claims specialists and other professionals across the country and handle millions of property and casualty, workers' compensation, disability, and other liability claims annually. Membership is comprised of independent claims adjusters and third-party administrator organizations, many of whom handle claims administration responsibilities for California insureds and their carriers. ACP member companies employ thousands of adjusters in the State of California and manage billions of dollars of claims for California insurers and policyholders.

Resolve Potential Consumer Confusion over Conflict of Law.

As shared in our March 8, 2019 submission, there are a number of existing California laws that appear to create competing obligations for our industry and others, including the California Insurance Code, Labor Code, and health laws. With that said, Section 1798.196 of the CCPA



provides that “[t]his title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.” The Act further provides that “[t]he obligations imposed on businesses by this title shall not restrict a business’ ability to ... comply with federal, state, or local laws... or exercise or defend legal claims.” Section 1798.145(a)(1), (4). The Act then specifically calls out a limited number of statutory scenarios in which the CCPA would not apply, including under the Confidentiality of Medical Information Act, Health Insurance Portability and Accountability Act, Fair Credit Reporting Act, and Gramm-Leach-Bliley Act, as well as clinical trials.

The imprecise language in the proposed regulations could be misconstrued to undercut this foundational principle. Respectfully, revisions are warranted. By way of example, the proposed regulations reference the conflict of law issue in guidance on responding to verified consumer requests to know, providing:

If a business denies a consumer’s verified request to know specific pieces of personal information, in whole or in part, **because of a conflict with federal or state law, or an exception to the CCPA**, the business shall inform the requestor and explain the basis for the denial...

Section 999.313(c)(5) (emphasis added). However, similar language is missing from that section’s guidance on responding to verified consumer request to delete.

In cases where a business denies a consumer’s request to delete the business shall do all of the following:

- a. Inform the consumer that it will not comply with the consumer’s request and describe the basis for the denial, including any statutory and regulatory exception therefor;
- b. Delete the consumer’s personal information that is not subject to the exception; and
- c. Not use the consumer’s personal information retained for any other purpose than provided for by that exception.

Section 999.313(d)(6).

To avoid confusion, we respectfully request that this Section reinforce that such requests can be denied “because of a conflict with federal or state law, or an exception to the CCPA.” Section 999.313(d)(6)(a) should be amended to read:

In cases where a business denies a consumer’s request to delete the business shall do all of the following

- a. Inform the consumer that it will not comply with the consumer’s request and describe the basis for the denial, including any

statutory and regulatory exception therefor if there is a conflict with federal or state law, or an exception to the CCPA.

Greater Clarity on the Interplay of “Businesses” and “Service Providers”

The proposed regulations could also be misread to impede members’ ability to duly carry out their lawful responsibilities. ACP companies respond every day to individuals and businesses who suffer a loss such as a workplace injury, property or casualty damage, or liability. Insurance carriers and self-insured companies retain our member companies for expert advice and knowledge throughout the management of claims entrusted to their care. ACP companies provide a full range of claims services from claims adjusting to comprehensive claims management. ACP focuses on the importance of claims specialists as front line responders when an individual or business suffers a loss such as a workplace injury, property or casualty damage, or liability. For claimants, ACP companies help individuals and companies begin to recover from such a loss. For carriers and self-insured customers, ACP companies are a strategic business partner and trusted advisor providing professional claims services integral to risk management. At each step of this process, important information is shared to facilitate effective and efficient claims management.

Given these important roles and responsibilities, and to ensure the most expedient claims management and administration, while avoiding consumer confusion and consternation, there are adjustments that should be made to the proposed regulations’ guidance on Service Providers. In particular, Section 999.314 should be revised to bring more clarity to who qualifies as a service provider and what their duties are under the Act.

- Subsection (a) states a person or entity that provides services to a person or organization that is a service provider to also be a service provider under the law. More concrete detail is needed to define those relationships. For example, does a service provider pass on deletion requests to its own service providers, or does the business, as the CCPA text seem to indicate, have the responsibility to direct each and every service provider in the provision chain?
- Subsection (c) states that a service provider “shall not use personal information received from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity.” There is, however, a carve out for service providers’ combining personal information received from one or more entities “to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.” To reduce confusion about the ability to share information between claimants and carriers, and remove unnecessary barriers to appropriate information sharing, the subsection should be revised to also allow the following sharing: “A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, ~~or~~ protect against fraudulent or illegal activity, complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or otherwise perform



**association of
claims professionals**

a contract between the business and the consumer, as well as where the combination is reasonably anticipated within the context of the service provider's business purpose."

- Subsection (d) requires service providers that receive a request to know or delete from a consumer to "explain the basis for the denial" if the service provider does not comply with the request and to inform the consumer that the consumer should submit the request directly to the business. This provision would seem to impermissibly expand the Act's reach to require service providers to comply with obligations otherwise resting with "business." In addition, compliance with such a new standard would be unduly burdensome and create confusion about where the line should be drawn between service providers and businesses on request management. It should therefore be removed.

ACP appreciates the opportunity to provide comments on the proposed regulations. If you have any questions concerning our comments, or if we can be of further assistance, please contact Susan Murdock at [REDACTED]. We thank you for consideration of these comments and welcome any further questions you may have.

Sincerely,

Susan R. Murdock
Executive Director
Association of Claims Professionals
1700 Pennsylvania Avenue, Suite 200
Washington, DC 20006
Phone: [REDACTED]
www.claimsprofession.org



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

RE: Preliminary Rulemaking Activities related to The California Consumer Privacy Act

Ladies and Gentlemen:

The Association of Claims Professionals (ACP) is pleased to respond to the request for comment on the Preliminary Rulemaking Activities related to The California Consumer Privacy Act (CCPA). While ACP members are strong proponents of individual privacy rights, we have significant concerns that the unintended application of the CCPA to claims professionals will cause widespread confusion and discord among California consumers and result in conflicting regulatory standards for our members. As such, for the reasons below, we ask the California Department of Justice to clarify the intent of the legislature that the CCPA does not apply to the activities of independent claims professionals.

ACP's Interest in Preliminary Rule Making Activities

ACP (formerly known as the American Association of Independent Claims Professionals or AAICP) was formed in 2002 as the only national association representing the interests of the nation's independent claims professionals. ACP members employ thousands of claims specialists and other professionals across the country and handle millions of property and casualty, workers' compensation, disability, and other liability claims annually. Membership is comprised of independent claims adjusters and third-party administrator organizations, many of whom handle claims administration responsibilities for California insureds and their carriers. ACP member companies employ thousands of adjusters in the State of California and manage billions of dollars of claims for California insurers and policyholders.

Comments on the CCPA

- I. The Department Should Clarify that the Claims Adjusting Industry is Exempt from the CCPA.**
 - 1. The California Insurance Code, Labor Code, and health laws extensively regulate the claims adjusting industry in the area of transparency and privacy and already provide greater protection specific to insured consumers.**



The CCPA was intended to fill in gaps in California privacy law, which is why the California legislature believes existing law should be construed to harmonize with the CCPA *if possible* but preempts the CCPA in the event of a conflict.¹ Moreover, California has specifically and comprehensively addressed transparency and privacy in the claims adjusting industry in a manner that provides greater protection to the consumer than what will be afforded under the CCPA when it is implemented. Given this extensive existing regulation, the Department should clarify that the CCPA does not apply to the claims adjusting industry to avoid conflicting regulation, an uncertain preemption analysis, and to protect consumers.

Perhaps most notably, the California Insurance Information and Privacy Protection Act (IIPPA) regulates the claims management industry as “Insurance Support Organizations” in the context of certain insurance transactions for substantially the same purpose as the CCPA.² Indeed, not only are the purposes of the IIPPA substantially similar to the CCPA, but the protections contained within the IIPPA mirrors if not exceed much of the CCPA. For example, insurance institutions or agents must provide a “notice of information practices” upon delivery of a policy or collection of personal information that includes all of the information the CCPA would require *plus* the investigative techniques used to collect such information. Not only that, but California insureds already have rights pursuant to the IIPPA to access, amend, correct, and delete certain information in a manner that actually makes sense in the insurance context.³

Other aspects of the California Insurance Code, Labor Code, and health laws have also required transparency and privacy protection for years. Administrators must provide written notice explaining its relationship with the insurer and policyholder “agents of insurers” and face criminal penalties for unauthorized disclosure of confidential information. The Labor Code severely limits what medical information may be disclosed when processing worker’s compensation claims.⁴ Relatedly, where the CCPA allows requests for the disclosure of relationships with third parties related to a consumer’s personal information, the Insurance Code already requires administrators to provide written notice advising insured individuals of the identity of details regarding the relationship between the administrator, policyholder,

¹ See Cal. Civ. Code §1798.175.

² See Cal. Ins. Code § 791 (“[T]o establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance-support organizations; to maintain a balance between the need for information by those conducting the business of insurance and the public’s need for fairness in insurance information practices, including the need to minimize intrusiveness; to establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information for the purpose of verifying or disputing its accuracy; to limit the disclosure of information collected in connection with insurance transactions; and to enable insurance applicants and policyholders to obtain the reasons for any adverse underwriting decision.”); Cal. Ins. Code § 791.02 (defining “insurance support organization”).

³ See Cal. Ins. Code § 791.08. Similar to the CCPA, access requests must be honored within 30 days, although unlike section 1798.100(d), the IIPPA allows a reasonable fee for the expenses incurred, which is not a difference in the level of privacy protection but rather a reasonable business practice. See Cal. Ins. Code §791.10.

⁴ See Cal. Ins. Code §§ 1759.9, 1877.4; Cal. Lab. Code § 3762.



and insurer.⁵ In the context of workers compensation insurance, “agents of insurers” are obligated to keep information confidential and face criminal penalties for unauthorized disclosure of such information.⁶

As referenced above, in addition to the Insurance Code the California Labor Code also limits disclosure of medical information insurers and third party administrators retained by self-insured employers to administer workers’ compensation claims receive to: (1) medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition; and (2) medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.⁷ Again, these protections are greater than those which will be afforded by the CCPA, arguing in favor of a blanket exemption from the CCPA for independent claims adjusters.

Beyond both the Insurance and Labor Codes, a third law -- the Confidential Medical Information Act (CMIA) -- also restricts the use and disclosure of any medical information claims professionals receive. For example, “[n]o person or entity engaged in the business of furnishing administrative services to programs that provide payment for health care services shall knowingly use, disclose, or permit its employees or agents to use or disclose medical information possessed in connection with performing administrative functions for a program, except as reasonably necessary in connection with the administration or maintenance of the program, or as required by law, or with an authorization.”⁸ Further, when claims professionals (“that provide[] billing, claims management, medical data processing, or other administrative services for providers of health care or health care service plans or for insurers, employers, hospital service plans, employee benefit plans, governmental authorities, contractors, or other persons or entities responsible for paying for health care services rendered to the patient receive medical information from health care providers and health care service plans”) receive medical information from health care providers or health care service plans, they cannot further disclose the information in a way that would violate the CMIA.⁹

California has already enacted a significant body of law to increase transparency for and protect the privacy of insured California consumers. If the CCPA was interpreted to apply to the claims adjusting industry the result would be a complicated patchwork quilt of regulation that lessens, rather than increases, consumer privacy. Further, application of the CCPA to the claims management industry would result in uneven application of the law given that each company would need to apply a complicated preemption analysis to nearly every right in the CCPA and decide if existing law or the CCPA is more stringent in the particular scenario.

⁵ See Cal. Ins. Code § 1759.9.

⁶ See Cal. Ins. Code § 1877.4.

⁷ See Cal. Lab. Code § 3762.

⁸ Cal. Civ. Code § 56.26(a).

⁹ See Cal. Civ. Code § 56.10(c)(3).

2. Where the CCPA may be said to apply, the law already contains explicit exceptions for key aspects of the claims adjusting industry, creating confusion for consumers.

The application of the CCPA to the claims adjusting industry will result in widespread consumer confusion without providing additional privacy or transparency protections. Where the law could arguably be read to apply, the CCPA exempts nearly all of the personal information the claims management industry receives in order to process claims: medical information governed by the CMIA, protected health information (PHI) collected as a business associate under HIPAA, information collected as part of a clinical trial, information in consumer credit reports, and in some cases, financial information disclosed pursuant to federal and California law. It is unclear and debatable whether any remaining information that does not fit neatly into the above exempt categories would be subject to CCPA obligations.

Further, claims management activities will constantly trigger CCPA exceptions, particularly when it comes to deletion requests directly from consumers or indirectly from businesses subject to the CCPA. The application of exceptions, which are needed to comply with existing law, will create confusion and likely frustration for consumers trying to exercise CCPA rights.¹⁰ For example, administrators will be exempt from deleting information related to transactions they are required to maintain confidentially in books and records and make available to insurers for at least five years pursuant to existing legal obligations.¹¹ In other words, insureds that lodge deletion requests in accordance with the CCPA rather than the proper procedure for the insurance context provided by the IIPPA will fall within an exception and therefore be rendered meaningless. This is why in addition to drafting the legal obligation exception to deletion requests, the CCPA repeats that the law is not intended to restrict the ability to comply with other laws.

As noted above, wherever the CCPA may be stretched to cover any remaining claims management activities that are not already facially exempt based on the category of information, the law will nevertheless constantly provide exception. Not only does this create a genuine question for members of the claims adjusting industry as to whether the CCPA is relevant to them, but it will undoubtedly create confusion and likely frustration for consumers and CCPA-regulated businesses that may not understand why the industry is exempt from complying with so many of their requests. To avoid both outcomes, the Department should issue a clear statement exempting the independent claims adjusting industry from the scope of the CCPA.

¹⁰ The most common exceptions will include (1) to complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer; (2) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; (3) to comply with a legal obligation; or (4) to otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. See Cal. Civ. Code §1798.105(d).

¹¹ See Cal. Ins. Code § 1759.3.

3. The California legislature did not intend the CCPA to further regulate the pro-consumer claims adjusting industry; the Department should make that explicitly clear.

The preamble to the CCPA emphasizes the intent of the California legislature to create privacy protections in response to business practices proliferated by the age of big data, while acknowledging existing law has already provided such protection in various other contexts. California had the same concerns regarding transparency and privacy protection in the claims management and broader insurance industry and intentionally addressed these concerns effectively throughout the state's legal code. Claims adjusters are specifically covered by existing law. The adjusting industry works on behalf of individuals and businesses in times of need, such as the recent California wildfires, delivering an estimated \$45 billion each year in claims payments. It would be deeply unfortunate if the CCPA were to unintentionally sweep up claims adjusters and double-regulate the industry, likely lessening today's existing protections. These unnecessary gray areas would disrupt functioning privacy compliance programs in the claims industry and even worse, burden claims recovery efforts from proceeding as quickly and smoothly as possible. It is clear that the California legislature intended the CCPA to exempt claims adjusters -- the Department's regulations should remove any ambiguity and clearly reflect that intent.

ACP appreciates the opportunity to provide comments on the Preliminary Rulemaking Activities related to the CCPA. If you have any questions concerning our comments, or if we can be of further assistance, please contact Susan Murdock at [REDACTED]. We thank you for consideration of these comments and welcome any further questions you may have.

Sincerely,



Susan R. Murdock
Executive Director
Association of Claims Professionals
1700 Pennsylvania Avenue, Suite 200
Washington, DC 20006
Phone: [REDACTED]
www.claimsprofession.org