



State of California
Office of the Attorney General

ROB BONTA
ATTORNEY GENERAL

November 21, 2022

Submitted via Federal eRulemaking Portal

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Docket ID: Commercial Surveillance ANPR, R111004

Dear Commissioners and Staff:

I write to comment on the Federal Trade Commission's (FTC) advance notice of proposed rulemaking on the prevalence of commercial surveillance and data security practices that harm consumers.¹ The California Attorney General's Office has engaged in extensive consumer privacy enforcement and has developed a deep fund of knowledge concerning commercial surveillance practices and data security through its enforcement of the California Consumer Privacy Act (CCPA), the only operative comprehensive privacy rights framework in the country, among other consumer laws. I appreciate the opportunity to share my Office's experience with the Commission, and I urge the Commission to use its regulatory authority to protect consumer privacy by defining and prohibiting additional forms of unfair and deceptive acts and practices related to data privacy protection, as described below. Such regulations would provide a critical floor of privacy protection, while preserving the demonstrated ability of the states to innovate and respond to evolving technologies in the protection of consumer privacy.

Executive Summary

Based on my Office's experience enforcing California's privacy laws, including the CCPA and others, I urge the Commission to promulgate regulations that:

¹ I share the concerns articulated by the Attorneys General that filed a separate multistate comment letter. See Cmt. of Mass. Atty. Gen. Off. (Nov. 17, 2022) <<https://www.regulations.gov/comment/FTC-2022-0053-0764>>.

- Establish guardrails to protect particularly sensitive personal information, such as precise geolocation and biometric information;
- Provide consumers with a right to opt-out of the sale of their personal information by data brokers, and by businesses that collect and sell consumer personal information without any direct relationship to the consumer;
- Prohibit businesses and operators of third-party online trackers from tracking or selling the data of users that have enabled privacy controls that signal that the consumer rejects commercial surveillance practices;
- Require online services and products that are likely to be accessed by children to have a more stringent age verification process commensurate with the potential harm that could arise from a child accessing the service or product;
- Require businesses that collect or maintain health information from consumers, but that are exempt from federal health information privacy laws, to have reasonable security; and
- Protect vulnerable patients from algorithmic decision-making tools in the healthcare and insurance industry that perpetuate unfair discrimination.

Background on California's Privacy Regulation and Enforcement

California has long been at the forefront of consumer privacy regulation and enforcement. As home to both Silicon Valley and Silicon Beach, California has led the nation, passing the first data breach notification law in 2003; requiring operators of online services to post privacy policies beginning in 2004; and giving consumers core privacy rights to access, delete, and stop the sale of their data in 2018. Every state now has a data breach notification law, and other states are following California's lead by moving to enact comprehensive privacy frameworks. California has also innovated in the absence of federal regulation, such as by requiring additional protections for patient privacy in its Confidentiality of Medical Information Act (CMIA), including those that apply to the operators of mobile applications. Most recently in September of this year, the Golden State enacted the California Age-Appropriate Design Code Act, (Assembly Bill 2273), which requires businesses to consider the best interest of child users and to default to privacy and safety settings that protect children's mental and physical health and wellbeing.

Through our recent privacy investigations, rulemakings, and enforcement actions, the California Attorney General's Office has developed insights regarding commercial surveillance and data security that inform the recommendations that follow. For example, our investigation of and lawsuit against cosmetics retailer Sephora for violations of the CCPA provided visibility into the utility of enabling consumers with tools to assert opt-out rights easily and effectively,

including through a global control.² In our case against Equifax for its failures following a massive data breach, we and our sister states advanced critical requirements for reasonable data security safeguards after half of the country’s adult population had their Social Security number compromised.³ And in our case against Glow, we established that operators of mobile applications have specific obligations to protect Californians’ sensitive reproductive and sexual health data, regardless of whether they are covered by federal health privacy laws.⁴ All of these cases were brought at least in part under California’s Unfair Competition Law, and alleged that the defendants had engaged in unlawful, unfair, or deceptive business acts and practices.

THE COMMISSION SHOULD PROMULGATE REGULATIONS THAT CODIFY NEW UNFAIR OR DECEPTIVE ACTS BASED ON PREVALENT, HARMFUL PRACTICES INVOLVING COMMERCIAL SURVEILLANCE OF CONSUMERS.

1. **The notice-and-consent framework does not effectively protect consumer privacy, and it improperly places the burden on consumers to protect themselves from surveillance practices controlled by business. The Commission should require businesses to minimize the collection of data and outright prohibit the collection and use of some forms of sensitive information as an unfair business practice.**

Notice and consent has been the dominant legal framework for online data collection practices. In 2004, California began requiring operators of online services to post a conspicuous privacy policy on their data collection and sharing habits. Deepening this requirement, the CCPA mandates that businesses provide notice at or before the point of collection of any personal information.⁵ Businesses typically treat a consumer’s continued use of a service functions as providing implicit consent to all of the business’s information practices. Although it has been the model for data collection, this “notice-and-consent” framework has been profoundly ineffective at protecting consumers’ privacy rights.

Though ubiquitous, privacy policies have become lengthy, unreadable documents drafted by lawyers, typically for lawyers, and not readily reviewed or understood by consumers.⁶

² Compl., *People v. Sephora, Inc.* (Super. Ct. S.F. City and County, 2022, No. CGC-22-601380) <<https://oag.ca.gov/system/files/media/pea-sephora-complaint.pdf>>.

³ Compl., *People v. Equifax, Inc.* (Super. Ct. S.F. City and County, 2019, No. CGC-19-577800) <<https://oag.ca.gov/system/files/attachments/press-docs/Equifax%20Complaint.pdf>>.

⁴ Compl., *People v. Upward Labs Holdings, Inc. & Glow, Inc.* (Super. Ct. S.F. City and County, 2020, No. CGC-20-586611) <<https://oag.ca.gov/sites/default/files/2020%2009-17%20-%20People%20v%20Upward%20Labs%20-%20Complaint.pdf>>.

⁵ The CCPA was passed by the legislature in 2018, then subsequently amended by the Consumer Privacy Rights Act (CPR) after voters approved the ballot measure in November 2020.

⁶ Or sometimes, the policies reflect that it was written by someone with a keen sense of humor, such as this one by Security.org in which it included, “We may reserve the right to claim naming rights of your firstborn child at a time chosen by ourselves.” Griffith, *Everyone Wants Data Privacy But No One Reads Privacy Agreements*, PC Mag (Apr. 19, 2021) <<https://www.pcmag.com/news/everyone-wants-data-privacy-but-no-one-reads-privacy-agreements>>. McDonald & Cranor, *The Cost of Reading Privacy*

Businesses produce pages-upon-pages of privacy policies that are often both convoluted *and* vague, full of legalese, and that purport to provide flexibility to the business to permissively collect everything by stating what the company “may” do – as in, “we may collect all of your stored contacts.” Other policies are so comprehensive that the consumer never knows which parts apply to them or their data. Large corporations may use the same policy for each of their subsidiaries and disclose, for example, that they use consumer personal information across their portfolio; yet many consumers fail to realize that by consenting to use by one business they are consenting to a sprawling array of affiliates.⁷ And in an attempt to be succinct, some policies lack any specificity such that a consumer is left without realizing that, for example, consumer personal information which is collected for “marketing” can be used for both online targeted advertising *and* mailed advertisements after companies cross-reference from other sources to confirm a website user’s matching physical address.⁸ How a business collects and uses data can be complicated and, in some cases, outright shocking.⁹ But the law has not caught up to prohibit even the most pervasive data collection and utilization practices.

Businesses avoid liability for how data is collected and used because consumers are typically deemed to have given consent to the spectrum of uses described in terms of service, privacy policies, and similar disclosures. Compounding the problem of ineffective notices are deceptive mechanisms or dark patterns that improperly force users into actions that appear to communicate consent to egregious privacy practices,¹⁰ as well as websites that intentionally make it difficult for the user to reject data collection so that the sites can continue online tracking.¹¹ Even in the European Union, with stringent General Data Protection Regulation

Policies (2008) I/S: A Journal of Law and Policy for the Information Society 4 no. 3, 540, 543 (in 2008, reading every privacy policy will require 244 hours per year).

⁷ Match.com Privacy Policy <<https://www.match.com/legalpolicy/privacypolicy>>.

⁸ Companies may share online data on its website visitors with other companies who send targeted advertisements in the mail to the consumer. Kelly, *You’ve Got Snail Mail: Targeted Online Ads are now Literally Following you Home*, Wash. Post (Jan. 30, 2020) <<https://www.washingtonpost.com/technology/2020/01/30/junk-mail-targets-ads/>>.

⁹ For example, Grindr, an online dating service, sold location data to third parties, which led to outing a Catholic priest as gay. Clark, *Brokered Cell Location Data Led to the Outing and Resignation of a Catholic Official*, The Verge (Jul. 20, 2021) <<https://www.theverge.com/2021/7/20/22586161/cell-phone-location-data-grindr-catholic-church-report-data-brokers>>. Another prominent example is the Cambridge Analytica scandal, which involved data collected about the friends of Facebook users who took quizzes, and that data was then used to create voter profiles. Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. Times (Apr. 4, 2018) <<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>>.

¹⁰ See Medine & Murphy, *Nobody Reads Privacy Policies: Why We Need to Go Beyond Consent to Ensure Data Privacy*, Next Billion (Dec. 16, 2019) <<https://nextbillion.net/beyond-consent-for-data-privacy>>; Fowler, *I Tried to Read All My App Privacy Policies. It was a Million Words*, The Washington Post (Mar. 31, 2022) <<https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies>>.

¹¹ Unfortunately, the proliferation of cookie banners has become both a nuisance for many consumers as well as another way for businesses to obtain “consent” via deceptive tactics. Lomas, *Hold-outs Targeted in Fresh Batch of Noyb GDPR Cookie Consent Complaints*, TechCrunch (Aug. 8, 2022)

(GDPR) requirements for obtaining consent that is “freely given, informed, specific and unambiguous” (GDPR, recital 32), consumers routinely click past cookie banners with little thought to what they are agreeing to because the cookie banners stand in the way of the product or service they wish to access. In other cases, obtaining meaningful consent is unlawfully thwarted; for example, noyb (None of Your Business), a private advocacy group, identified and then filed 270 complaints in this year alone against online businesses that use deceptive cookie banners.¹² Thus, even an opt-in regime that requires express consent is not immune to notice fatigue, and is not always sufficient to protect consumers from unlawful business collection, or alternatively, to deter businesses from deceptive acts and practices.

In the United States, however, businesses need no express opt-in or meaningful consent for collection; at least as to consumers over the age of 13, businesses are free to collect with limited restraint.¹³ Businesses treat consent to terms as having been given through a consumer’s continued use of the product or service, even if the user is merely browsing a website.¹⁴ Consent is also typically all-or-nothing: a consumer uses the product, and through that use they are treated as having consented to all data collection, retention, and disclosure practices. Consent to a first-party businesses’ collection of data has also been stretched to encompass data collection and use by downstream entities, with those entities contending that a consumer reasonably expected third-party collection and use.¹⁵ The result of the notice and consent framework is that businesses have an incentive to provide broad disclosures that immunizes the practice of collecting and retaining as much consumer data as possible, notwithstanding security risks to the business and potential actual harms to the consumers.

a. The burden should not be on consumers to protect themselves from businesses’ surveillance practices. It should be shifted to businesses through requirements that they minimize data collection and use data for limited purposes.

<<https://techcrunch.com/2022/08/08/noyb-gdpr-cookie-consent-complaints/>>; Nocera, *How Cookie Banners Backfired*, N.Y. Times (Jan. 29, 2022)

<<https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html>>.

¹² For example, a website may hide a “reject all” cookies option or make the user click through multiple links to reach that option. This frustrating design would nudge a user into consenting to tracking even though they would not do so if the “reject all” option was more clearly presented. See Lomas, *More Deceptive Cookie Banners Targeted in Latest Noyb EU Action*, TechCrunch (March 4, 2022)

<<https://techcrunch.com/2022/03/04/noyb-second-cookie-complaints/>>.

¹³ Children’s Online Privacy Protection Act, 15 U.S.C. § 6502, subd. (a)(1).

¹⁴ See, e.g., Twitter, Privacy Policy (June 10, 2022) <<https://twitter.com/en/tos>> (“By using the Services you agree to be bound by these Terms.”); Washington Post, Privacy Policy (July 1, 2022) <<https://www.washingtonpost.com/privacy-policy/>> (“Your use of the Services or your provision of information to us following such changes indicates your acceptance of the revised Privacy Policy.”).

¹⁵ For example, Kochava, a location data broker, argued that consumers using mobile apps agree to share their location, even sensitive locations, and thus the company should not be liable if third-parties that buy Kochava’s location data subsequently identify the individual user. See Compl. at par. 19, *Kochava, Inc. v. FTC* (D. Id. 2022) (No. 2:22-cv-00349).

California's recent actions have put it on a new path that moves away from perfunctory legal hurdles or meaningless, confusing consent banners. Based on principles of data minimization and purpose or use limitations, the recent amendments to the CCPA include language that shifts the burden from consumers to businesses, and by requiring businesses to collect only what is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed[.]"¹⁶ Data minimization concepts have also appeared in proposed draft regulations by the California Privacy Protection Agency that advanced these amendments to the CCPA.¹⁷ Moving away from the default of "collect everything" requires providing businesses with an incentive to minimize their collection, retention, and use of data, and to develop business practices that advance rather than diminish consumer privacy. Requiring businesses to obtain consent to data collection that goes beyond a traditional notice and consent model, requiring consent that is specific, granular, and freely given, and prohibiting business from conditioning the provision of goods or services on sweeping access to consumer data, may also positively shift consumer behavior, such that the times in which a consumer is asked for consent, they can actually consider the benefits and risks of allowing that entity to collect their data. It would also disincentivize businesses from retaining data long past when it is necessary for the purpose for which it was collected, which increases the risk that the data will be exposed in a data breach.¹⁸ Businesses certainly should not be retaining data indefinitely.¹⁹

¹⁶ This text will be codified as California Civil Code Section 1798.100, subdivision (c). West's Ann. Cal. Civ. Code, § 1798.100, subd. (c). See also United Kingdom Information Commissioner's Office (UK ICO), *Purpose Limitation, Data Minimisation, and Storage Limitation* <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/purpose-limitation-data-minimisation-and-storage-limitation/>>.

¹⁷ Cal. Priv. Prot. Agency, Text of Proposed Regulations (Nov. 3, 2022), §§ 7002-7004 <https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf>. For example, the proposed regulations set forth specific guidelines on how a business may collect, use, retain, and/or share personal information for purposes beyond a consumer's reasonable expectation by requiring meaningful, explicit consent; notably, that a business cannot obtain consent by bundling choices so that a consumer must consent to additional uses of their personal information in order to use the product.

¹⁸ For example, the FTC's 2019 complaint against InfoTrax noted the company's failure to have a systematic process to inventory and delete consumer personal information that was no longer needed was an unreasonable security practice that led to multiple and repeated data breaches. See Compl. at par. 10, *In the Matter of InfoTrax Systems, L.C.*, F.T.C. File No. 162-3130 (Dec. 30, 2019) <https://www.ftc.gov/system/files/documents/cases/c-4696_162_3130_infotrax_complaint_clean.pdf>.

¹⁹ Retaining data indefinitely poses risk to both the consumer and to the business. See, e.g., Hill, *The T-Mobile Data Breach: A Timeline*, CSO (Aug. 27, 2021) <<https://www.csoonline.com/article/3630093/the-t-mobile-data-breach-a-timeline.html>> (T-Mobile data breach affecting approximately 7.8 million current customers and 40 million former or prospective customers); Fed. Trade Comm'n, "FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers" (Oct. 24, 2022) <<https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>> (FTC settlement with company that was alerted to security failures years before a data breach but failed to take appropriate actions to either fix the security flaws or delete unnecessary data).

The FTC should issue regulations affirming these ideas. The FTC can and should make the regulatory declaration that:

A business has committed an unfair or deceptive act or practice if it collects, uses, or retains personal information in a way that is not reasonably necessary and proportionate to the purposes for which the personal information was initially collected or processed. A business shall obtain explicit, informed consent²⁰ before collecting or using personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information was initially collected or processed. A business shall not obtain explicit consent by requiring a consumer to consent to an additional unrelated or incompatible purpose in order to use the product.

b. The FTC should place additional guardrails around the collection or use of sensitive personal information, such as precise geolocation and biometric information.

In addition, basic guardrails need to be established around the collection and use of sensitive personal information, including at a minimum, precise geolocation and biometric information. Four points of geolocation information can easily identify an individual, reveal sensitive details about the individual's movements that could disclose deeply intimate moments—home, office, erectile dysfunction doctor, pharmacy²¹—and allow companies to make inferences for their own commercial interests.²² Biometric information, such as fingerprints or a person's face, are unique and cannot be reset. More and more companies have been collecting both types of information and sharing or using the data for unexpected purposes, often without consumers' knowledge.²³ Mobile apps frequently collect and trade location data with data brokers in exchange for analytics, and wearable and mobile device providers may further monetize their users through the collection and sale of geolocation and other sensitive

²⁰ In defining “explicit, informed consent” for purposes of such a regulation the Commission might consider the draft CPRA regulations recently promulgated by our colleagues at the California Privacy Protection Agency. See Cal. Priv. Prot. Agency, Text of Proposed Regulations (Nov. 3, 2022), § 7004.

²¹ Other examples of sensitive locations could include cancer treatment facilities, substance abuse centers, mental health centers, weight loss centers, and domestic violence or homeless shelters.

²² Thompson & Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019) <<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>>.

²³ For example, the FTC recently filed a complaint against Kochava, a data broker that collected and sold consumer location information obtained from mobile apps. Fed. Trade Comm'n, “FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations” (Aug. 29, 2022) <<https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other>>.

information.²⁴ Consumers should not have to give up sensitive personal information and lose their anonymity just by venturing into public spaces.

A rule prohibiting companies from collecting, using, retaining, or sharing sensitive personal information in a way that a reasonable consumer would not expect would reinforce previous Commission settlements, like those in the groundbreaking Flashlight App²⁵ and Everalbum cases.²⁶ The FTC should codify the algorithmic disgorgement requirement in the Everalbum settlement so that when consumers upload data for one purpose and the business uses it to develop a separate product, model, or algorithm that those consumers would not have expected, the business has engaged in an abusive act or practice, and must delete that separate product, model, or algorithm. The FTC should similarly codify another provision of the Everalbum settlement, declaring that businesses engage in an unfair act or practice if they retain sensitive information after users delete their accounts.

The Commission should also prohibit the collection or use of certain forms of highly sensitive information as an unfair practice, regardless of user consent. The Commission should prohibit collection, retention or use of particularly sensitive geolocation data, including but not limited to data showing that a user has visited reproductive health and fertility clinics, places of worship, domestic violence shelters, and addiction recovery facilities.²⁷ Companies engaged in location tracking are capable of identifying and deleting information of this nature, and no reasonable consumer would think that they had consented to the tracking of their geolocation when they are visiting such locations. While some companies have voluntarily taken steps to stop collecting this information,²⁸ the tracking of consumers' geolocation at sensitive locations continues.

²⁴ Ng & Keegan, *Who is Policing the Location Data Industry?* The Markup (Feb. 24, 2022) <<https://themarkup.org/the-breakdown/2022/02/24/who-is-policing-the-location-data-industry>>.

²⁵ Fed. Trade Comm'n, "Android Flashlight App Developer Settles FTC Charges It Deceived Consumers" (Dec. 5, 2013) <<https://www.ftc.gov/news-events/news/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived-consumers>>.

²⁶ Fed. Trade Comm'n, "FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology" (May 7, 2021) <<https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology>>.

²⁷ Limited exceptions may be made for momentary retention of information solely necessary to provide emergency response services or for a business to identify that the consumer has visited a sensitive location and flag that information for deletion. See, e.g., Clark, *Google Will Start Auto-Deleting Abortion Clinic Visits from User Location History*, Verge (July 1, 2022) <<https://www.theverge.com/2022/7/1/23191965/google-abortion-privacy-policy-location-history-period-tracking-deletion>> (discussing Google's decision to delete a consumer's visit to sensitive locations from the user's location history soon after the company's system has identified the user visited a sensitive location).

²⁸ For example, Google recently began deleting location data from sensitive places that would otherwise have been stored as part of a user's Location History setting; likewise, two location data sellers, SafeGraph and Placer.ai, have recently committed to stop selling location data associated with reproductive health center locations. Kaye, *"Likely to Cause Substantial Injury:" Why the FTC Put*

It is time for the Commission to adopt a bright line rule that protects consumers from commercial surveillance in places where the collection of geolocation information would be patently unreasonable and no reasonable consumer would rationally consent to the retention of precise geolocation data. The Commission should make the regulatory declaration that:

Collecting, retaining, using, or disclosing a consumer's exact or precise geolocation at a location that demands the highest protection of a consumer's privacy²⁹ constitutes an unfair business act or practice.

In addition to protecting sensitive geolocation, the FTC should prohibit third-party businesses from collecting biometric information.³⁰ Companies that have no direct relationship with a consumer should not be permitted to collect, retain or use that consumer's biometric data, such as by scraping billions of facial images from the internet to create a searchable database for paying clients.³¹ In contexts such as this, no consumer can provide consent to have their data collected, and consumers cannot protect themselves from such collection short of going into seclusion.³² To address this issue, the Commission should declare that:

It is an unfair business act or practice if any business that does not have a direct commercial relationship with a consumer collects their biometric information.

2. Consumers need better tools to stop data brokers from selling their information because the prevalence and pervasiveness of downstream sales cause harm.

Third-party companies with no direct relationship to consumers are receiving, scraping, trading, and buying consumer personal information. Some third parties, such as data brokers, collect, link, repackage, and resell this personal information. In doing so, these data brokers create commercially available profiles drawn from multiple data sources that can reveal the most sensitive details of our lives. The commercial availability of detailed individual profiles, of the

Kochava in the Spotlight, Protocol (Sept. 6, 2022) <<https://www.protocol.com/enterprise/ftc-kochava-mobile-location-data>>.

²⁹ Such locations should be defined to include, without limitation, reproductive health and fertility clinics, places of worship, domestic violence shelters, and addiction recovery facilities.

³⁰ The FTC should further define what is and what is not biometrics information, and can consider language in existing state biometrics laws such as the Illinois Biometric Information Privacy Act.

³¹ Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020) <<https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>>. See also Whittaker, *Despite Controversies and Bans, Facial Recognition Startups are Flush with VC Cash*, TechCrunch (July 26, 2021) <<https://techcrunch.com/2021/07/26/facial-recognition-flush-with-cash/>>.

³² Although we believe it's better to prohibit these third-party businesses with no direct relationship with a consumer from collecting their biometrics entirely, in the alternative the FTC could consider a rule requiring the third-party businesses to obtain consumer consent before collecting. Such a rule would make it impractical for companies that rely on data scraping to obtain consumers' consent.

sort that were once only available to sophisticated law enforcement and intelligence agencies, is a profound intrusion on individual privacy. Data brokers have given predatory businesses, scammers, and even violent criminals access to sophisticated intelligence that they can use to target consumers.³³ At the least harmful, data brokers' business models are merely frustrating for consumers to counteract. For example, one data broker could release incorrect information about a consumer that proliferates hundreds of times over, making it both extremely difficult for consumers to correct the information and virtually impossible for a consumer to understand where the initial error occurred and fix it at the original source.³⁴ Other data brokers might take data gathered for credit referencing purposes and resell it for marketing purposes,³⁵ or make inferences about consumers (e.g., "Rural and Barely Making It"), thereby subjecting those consumers to unwanted marketing and potential scams.³⁶ But in more harmful iterations, data brokers have sold information that has led to unspeakable crimes.³⁷ In most cases, consumers have no discernible method to identify these data brokers or prevent their data from being sold.

Regulations should address both of these problems. To help consumers learn which data brokers have their personal information, the FTC should require that businesses be more transparent in their privacy policies and identify the specific data brokers to which they sell personal information. Even with the CCPA's requirement that businesses disclose the categories of third parties with whom they disclose personal information to, the specific entities that acquire

³³ For example, two marketing data brokers, Epsilon and KBM Group, agreed to pay a total of approximately \$192 million to settle a U.S. Department of Justice investigation that the companies sold consumer lists to a number of mass-mailing fraud schemes that targeted elder victims. United States Department of Justice, *Justice Department Recognizes World Elder Abuse Awareness Day; Files Cases Against Marketing Company and Executives who Knowingly Facilitated Elder Fraud* (June 15, 2021) <<https://www.justice.gov/opa/pr/justice-department-recognizes-world-elder-abuse-awareness-day-files-cases-against-marketing>>.

³⁴ Sherman, *Data Brokers are a Threat to Democracy*, *Wired* (Apr. 13, 2021) <<https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/>>.

³⁵ UK ICO, *Investigation into Data Protection Compliance in the Direct Marketing Data Broking Sector* (Oct. 2022) <<https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf>>.

³⁶ Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* (2014), <<http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>>.

³⁷ Judge Esther Salas was targeted as a federal judge and her family became the victim of an unthinkable crime when her son was murdered and her husband gravely injured after a shooter purchased her home address from a data broker. See Haworth, *Judge Salas Breaks Silence in Heartbreaking Video Tribute after Son's Shooting Death*, *ABCNews* (Aug. 3, 2020) <<https://abcnews.go.com/US/judge-salas-breaks-silence-heartbreaking-video-tribute-sons/story?id=72143701>>; Adams, *A Federal Judge Mourning her Son Calls for Increased Data Privacy*, *Marketplace Tech* (Aug. 6, 2020) <<https://www.marketplace.org/shows/marketplace-tech/federal-judge-esther-salas-gunman-attack-personal-information-data-privacy-online/>>. Troublingly, the CCPA does not protect publicly available personal information, meaning data brokers can sell information from government records, which may include someone's home address.

consumer data are unknown—and unknowable—to the consumer.³⁸ As a result, a business can merely state it sells personal information to “third parties” without explaining they are selling to “data brokers”, let alone “LiveRamp, Acxiom, Epsilon, Equifax, Experian, and CoreLogic.” To address this lack of transparency, the Commission should consider a rule that states:

It is an unfair business act or practice for a business to omit from its privacy policy the specific names of any data brokers that it sold or shared consumer personal information.

Even if a consumer knows which data brokers to contact, stopping the further sale of their personal information presents a challenge. Since 2014, the Commission recommended that Congress pass a law requiring data brokers to respect consumers’ choices to opt-out of the sale of their personal information.³⁹ But data brokers are not required to offer a mechanism for consumers to opt out of their sales. And nearly a decade has passed without congressional action; no national data broker registry exists where consumers could securely submit basic identifying information (e.g., name, phone number, date of birth) sufficient to stop the sale of their personal information by data brokers.⁴⁰

To address this persistent problem, the Commission should find that the lack of any opt-out mechanism from a data broker’s sale of personal information is an unfair practice:

*It is an unfair business act or practice for a company that sells a consumer’s personal information but has no direct commercial relationship with that consumer to not provide any mechanism for that consumer to stop the sale of their personal information.*⁴¹

3. **In the online context, the Global Privacy Control is already an effective tool for Californians to stop commercial surveillance, including by online trackers, and could be universally interpreted for all Americans as a choice to stop the sale of their data.**

³⁸ Cal. Civ. Code, § 1798.110. subd. (a)(2).

³⁹ Fed. Trade Comm’n, Data Brokers: A Call for Transparency and Accountability (May 2014) <<http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>>.

⁴⁰ California passed a data broker registry law in 2019 which allows consumers to view an online registry of existing data brokers. (Civ. Code, § 1798.99.80 et seq.) However, the registry has limited efficacy as with over 400 registered data brokers, consumers face a huge hurdle to go broker-by-broker and exercise the right to opt-out, especially as data brokers have very different processes and requirements to process the consumer’s request to opt-out.

⁴¹ As part of this proposed rule, the FTC may also want to consider regulations clarifying that data brokers may not use dark patterns that hinder consumer opt-outs. Mahoney, *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?* Consumer Reports (Oct. 1, 2020) <https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf>.

For over a decade, the FTC has warned about the privacy risks associated with third-party online tracking,⁴² but until recently, consumers could do little to effectively stop it. In that decade, use of online trackers has only become more common and more invasive as consumers conduct more of their daily business online. As a result, large technology companies have amassed detailed behavioral profiles on individuals—often unbeknownst to consumers that their data was invisibly collected to create these profiles.⁴³ Website and app developers install these online trackers, which permit third parties to surveil consumers’ behavior and access their data in exchange for personalized advertising or analytics services.⁴⁴

Industry efforts to engage in self-regulation have been lackluster. Trade groups advised that businesses “should provide consumers with the ability to exercise choice with respect to the collection and use of data for Online Behavioral Advertising purposes or the transfer of such data to [another entity] for such purpose[s].”⁴⁵ But that choice has mostly been a false one; businesses provide consumers with a take-it-or-leave-it choice, yet that choice proves meaningless when virtually every business engages in online tracking. Even when consumer tools did emerge, they proved ineffective⁴⁶ or, ironically, privacy invasive.⁴⁷ And industry-designed opt-out

⁴² Fed. Trade Comm’n, Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009) <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>>; see also Fed. Trade Comm’n, Cross-Device Tracking: A Federal Trade Commission Staff Report (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>.

⁴³ Apple’s introduction of a binary choice regarding app tracking had more of an impact than a decade of the advertising-industry created opt-outs of personalized advertising. See, e.g., Kantrowitz, *Apple’s Power Move to Kneecap Facebook Advertising is Working* (Sept. 24, 2021) CNBC <<https://www.cnbc.com/2021/09/24/apples-ios-changes-hurt-facebooks-ad-business.html>>.

⁴⁴ Brookman, *Understanding the Scope of Data Collection by Major Platforms*, Consumer Reports (May 2020) <https://digital-lab-wp.consumerreports.org/wp-content/uploads/2020/05/Understanding-the-scope-of-data-collection-by-major-platforms_2020_FINAL.pdf>; Cyphers & Gebhart, *Behind the One-Way Mirror: A Deep Dive into Corporate Surveillance*, Electronic Frontier Foundation (Dec. 2, 2019) <<https://www.eff.org/wp/behind-the-one-way-mirror>>.

⁴⁵ Digital Advertising Alliance, Self-Regulatory Principles for Online Behavioral Advertising (July 2009) <https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf>.

⁴⁶ For example, some businesses refused to honor consumer choice expressed via a “Do Not Track” signal. Edelman, *“Do Not Track” is Back and this time it Might Work*, Wired (Oct. 7, 2020) <<https://www.wired.com/story/global-privacy-control-launches-do-not-track-is-back/>>.

⁴⁷ Some of the tools for consumers to opt-out of the sale of their personal information require the consumer to turn on cookies in order to store the opt-out. But turning on cookies also allow other businesses to collect and store the consumer’s data. Sankin, *I Tried to Use the Ad Tech Industry’s Tool to Opt Out of Personalized Ads. Did It Work?*, The Markup (Mar. 25, 2021) <<https://themarkup.org/privacy/2021/03/25/i-tried-to-use-the-ad-tech-industrys-tool-to-opt-out-of-personalized-ads-did-it-work>> (“The cost is pretty high: Not only can these ad tech companies still collect data about me, but when I use Firefox, they can gather even more than they could before because I

mechanisms were confusing or not used by either businesses or consumers.⁴⁸ All of these initiatives fundamentally failed because they were merely voluntary and not legally mandated.

In California, businesses are required to let consumers easily opt out of certain forms of online tracking. In addition to granting a right to opt out of sale, the CCPA defines “sales” of personal information broadly as any exchange of personal information for anything of value.⁴⁹ This definition, subject to certain exceptions, covers transactions where first parties barter information about an individual’s online activities to a third party for services, like targeted advertising and analytics. When a first-party business engages in such online sales of personal information, the CCPA requires the business to post a “Do Not Sell My Personal Information” link on the business’s homepage,⁵⁰ which is intended to be easier for consumers to find and use than the industry-offered options.⁵¹ In actuality, however, the “Do Not Sell My Personal Information” link means that consumers seeking to effectuate their opt-out would have to visit and click the link on each first party business’s website, tediously going browser-by-browser or app-by-app, device-by-device.⁵² While the “Do Not Sell My Personal Information link” serves valuable purposes, such as by allowing businesses to offer an easy opt-out mechanism for offline sales of personal information, privacy-conscious consumers need better, easier options.

dramatically lowered my privacy settings in order to let the opt-out system function. The companies not participating in the opt-out can simply go hog wild. They can track me, load reams of personalize ads where I go. The works.”).

⁴⁸ One report released soon after Ad Choices was launched in 2010 described numerous problems with the program, including the fact that users were unable to opt-out of tracking by websites they were currently visiting because the opt-out only applied when the company was acting as a third-party behavioral advertising service, even participating companies had “infrequent compliance”, and the opt-out failed to extend to new companies that joined the program. Komanduri et al., *Ad Choices? Compliance with Online Behavioral Advertising Notice and Choice Requirements* (Mar. 30, 2011) Carnegie Mellon University

<https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab11005.pdf>. See also Cranor et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by the CCPA* (2020) 1, 3

<<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-cranor.pdf>> (noting that in tests, consumers still do not widely recognize the Ad Choices icon or the green Privacy Rights icon that DAA recommended for CCPA compliance).

⁴⁹ Cal. Civ. Code, § 1798.140, subd. (t).

⁵⁰ Cal. Civ. Code, § 1798.135, subd. (a).

⁵¹ For example, the Digital Advertising Alliance’s opt out program will not work on a browser like Firefox that, for consumer protection reasons, blocks third party cookies.

⁵² The struggle to opt-out can be likened to the struggle to read all the privacy policies of websites an average user visits in a year, which would be 244 hours per one researcher. See McDonald & Cranor, *The Cost of Reading Privacy Policies* (2008) *I/S: A Journal of Law and Policy for the Information Society* 4 no. 3, 540, 543; Cranor, Hoke, Leon & Au, *Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies’ Privacy Policies* (2014) TPRC Conference Paper.

Fortunately, the CCPA authorized the Attorney General to promulgate regulations that facilitate the consumer's submission of the opt-out.⁵³ To help consumers opt out as easily as businesses surveil, the regulations require businesses that collect personal information online to "treat user-enabled global privacy controls ... that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request [to opt out]."⁵⁴ Provisions similar to this regulation now appear in other states' comprehensive privacy laws.⁵⁵ This regulation is intended to, and in fact has, spurred innovation, prompting advocates and experts to develop the Global Privacy Control (GPC), which can be installed in web browsers and will repeatedly and instantaneously signal a consumer's opt out to every website they visit.⁵⁶ And to aid businesses in responding to the GPC, several privacy vendors offer off-the-shelf compliance solutions that process opt outs submitted via the GPC. In August 2022, the Attorney General's Office filed its first CCPA enforcement action, a stipulated final judgement with Sephora USA, Inc., after investigating the company's compliance with consumer requests to opt-out of the sale of personal information, including sales that made consumer personal information available to third-party entities via online tracking technology.⁵⁷ The Attorney General alleged, among other claims, that Sephora failed to comply with consumer requests to opt-out of these sales that were signaled via user-enabled global privacy controls, such as via the GPC. In addition to the announcement of the action against Sephora, the Attorney General provided further CCPA enforcement updates, including an ongoing enforcement sweep focusing on compliance with the GPC.⁵⁸

The FTC should require that businesses universally recognize a "do not sell" signal from a user-enabled global privacy control. Such a rule need not unduly burden businesses.⁵⁹ The

⁵³ Cal. Civ. Code, § 1798.185 (a)(4). The authority to promulgate regulations now sits with the California Privacy Protection Agency.

⁵⁴ Cal. Code Reg., tit. 11, § 7026, subd. (c).

⁵⁵ Col. Rev. Stat., tit. 6, art. 1, § 1306; Ct. Pub. Act No. 22-15, § 5.

⁵⁶ Global Privacy Control, Take Control of Your Privacy
<<https://globalprivacycontrol.org/#about>>.

⁵⁷ Cal. Atty. Gen. Off., "Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act" (Aug. 24, 2022)
<<https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement>>.

⁵⁸ *Ibid.*

⁵⁹ For example, companies would still be able to transmit personal information that a consumer intended to share (e.g., payment details to a bank or address to a delivery service). Businesses also could still hire service providers contractually obligated to only use personal information on behalf of the first party business, and not, for example, to build their own consumer profiles. Additionally, any rule should consider the technical complexity for identification—while an anonymous visitor to a website can have their personal information collected and sold to companies that can identify that person, such as via their IP address, a business should not be expected to opt out a user identified by their IP address from offline sales because processing the opt-out could be technically infeasible, or result in privacy invasions and other abuses. And, using the GPC as an example, businesses need only add a few lines of code to the website or app. Documentation available on the Global Privacy Control website indicates limited coding

Commission should consider defining a business's failure to process global opt-out signals as an unfair business act or practice. One option for this type of regulatory requirement is:

It is an unfair business act or practice for a business to sell or barter a consumer's personal information to a third party, if the consumer expressly signals via a user-enabled global privacy control, such as the GPC, that they do not want their data sold.

In addition, the Commission should consider a rule directed at the third-party recipients of consumer information, as these companies are generally much larger and direct the terms of their data collection on the first-party businesses. Additional language could prohibit third parties from willfully ignoring a detected opt-out signal in the course of engaging in a transaction that constitutes a sale.⁶⁰

4. Stringent age verification rules are necessary to address pervasive indifference to determining the age of online users and trigger heightened privacy protections for children.

To avoid complying with rigorous collection and use restrictions, online businesses eschew children's privacy requirements by employing subpar age verification methods.⁶¹ As a prominent example, most major social media platforms set a 13-year-old minimum age for users, but a recent survey indicates that approximately half of parents of children ages 10 to 12 and 32% of parents of kids ages 7 to 9 reported that their child used social media apps in the first six months of 2021.⁶² Unreliable age verification methods, such as self-verification, can be easily circumvented by children.⁶³ The resulting harms caused by weak age verification methods can be

to implement the GPC. Zucker-Scharff & Zimmeck, *How to Implement Global Privacy Control (GPC) for Publishers* <<https://global-privacy-control.glitch.me/>>.

⁶⁰ Third parties often have market dominance and can dictate the terms and adoption of their technology, but have a different compliance burden given the CCPA's framework between a consumer and a business. It is unfortunate that the legal framework reinforces a power dynamic in which third parties are not incentivized to assist the first-party business with its compliance obligations.

⁶¹ See, e.g., 16 C.F.R. §§ 312.2, 312.5(a)(1) (COPPA rules protecting children under age 13 from collection of data without parental consent); Cal. Civ. Code, § 1798.120, subd. (c) (CCPA provisions requiring opt-in consent to sell personal information of children under the age of 16).

⁶² Rodgers, *Children under 10 are using social media. Parents can help them stay safe online*, CNN (Oct. 18, 2021) <<https://www.cnn.com/2021/10/18/health/children-social-media-apps-use-poll-wellness/index.html>>; see also Moyer, *Kids as Young as 8 Are Using Social Media More Than Ever, Study Finds*, N.Y. Times (Mar. 24, 2022) <<https://www.nytimes.com/2022/03/24/well/family/child-social-media-use.html>>.

⁶³ See UK ICO, *Age Assurance for the Children's Code* (Oct. 14, 2021) p. 14 <<https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf>> (self-declaration "does not significantly mitigate risk as it is based on trust and can be circumvented, even if additional technical measures are applied."); *Children can bypass age verification procedures in popular social media apps by lying*, (Jan. 25, 2021) <<https://lero.ie/news-and-events/children-can-bypass-age-verification-procedures-popular-social-media-apps-lying>> (researchers found children of all ages can completely bypass age verification measures on most popular social media apps); Arthur, *'Major weaknesses' in*

significant.⁶⁴ When young children improperly access social media apps that are intended for teenagers and adults, for example, the consequences may range from persistent sleep deprivation⁶⁵ to sexual exploitation⁶⁶ and, in some cases, may result in serious physical harm or death of the child.⁶⁷ In order for any privacy framework regarding children's data to be effective at protecting children and their data, businesses must be required to accurately determine the age of its users⁶⁸ or alternatively, default to applying high levels of privacy when they have constructive knowledge that their audience is below a threshold age.

Adopting a privacy-protective way to determine a user's age without proving actual identity or requiring additional personal information is feasible. Technology solutions are

online alcohol sales age-verification controls, (Apr. 12, 2022)

<<https://www.beveragedaily.com/Article/2022/04/12/Major-weaknesses-in-online-alcohol-sales-age-verification-controls#>> (minors overcoming ineffectual age verification to purchase alcohol for delivery online).

⁶⁴ See Charmaraman et al., *Associations of early social media initiation on digital behaviors and the moderating role of limiting use* (Feb. 2022)

<<https://www.sciencedirect.com/science/article/abs/pii/S0747563221003769>> (paper showed that children 10 years old or younger who started use of Instagram or Snapchat were significantly associated with problematic digital behavior compared to children who started use later, including having online friends or joining social media sites parents would disapprove of, more problematic digital technology behaviors, more unsympathetic online behaviors, and greater likelihood of online harassment and sexual harassment victimization).

⁶⁵ De Montfort University, *DMU research suggests 10-year-olds lose sleep to check social media* (Sep. 16, 2022) <<https://www.dmu.ac.uk/about-dmu/news/2022/september/dmu-research-suggests-10-year-olds-lose-sleep-to-check-social-media.aspx>> (study found that 70 percent of a group of 10-year olds lost sleep from social media use).

⁶⁶ See e.g., Harwell, *A teen girl sexually exploited on Snapchat takes on American tech*, Wash. Post (May 5, 2022) <<https://www.washingtonpost.com/technology/2022/05/05/snapchat-teens-nudes-lawsuit/>> (lawsuit alleging man used Instagram and SnapChat to obtain sexually explicit images from female victim beginning when she was 12-year old and then distributed the images).

⁶⁷ See, e.g., Suliman, *Mother of 11-year-old who died by suicide sues social media firms Meta and Snap*, Wash. Post (Jan. 22, 2022) <<https://www.washingtonpost.com/nation/2022/01/22/selena-rodriguez-suicide-meta-snap-lawsuit/>> (law suit alleges that 11-year old's suicide was caused by defective design, negligence and unreasonably dangerous features of the defendant platforms); Clark, *The TikTok 'blackout challenge' has now allegedly killed seven kids / Parents say the app's algorithm showed their children deadly challenges*, The Verge (Jul. 7, 2022)

<<https://www.theverge.com/2022/7/7/23199058/tiktok-lawsuits-blackout-challenge-children-death>> (law suit allegations against defendant in multiple wrongful death suits involving death of children as young as 8 years old who engaged in self-strangulation attempting the "blackout challenge," after the platform showed them videos of other people trying it).

⁶⁸ See 5Rights Foundation, *But how do they know it is a child?* (Oct. 2021) p. 9 <https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf> (age assurance is empowering for child users because it offers "greater privacy, freedom from commercial pressures, content and information in formats and languages that they like, protection from misinformation or materials that promote harmful activities . . .").

emerging to estimate a user's age that do not require identifying the user.⁶⁹ For example, social media companies can cross-check accounts to confirm or disprove a user's stated age: if a user lists their age as 18 on a social media platform but has a friend sending them a "Happy Quinceañera" (15th birthday) message, it could flag inaccuracies in reported age.⁷⁰

In addition to improved age-verification techniques, companies cannot purposely avoid extrinsic indications that their user base includes children. Simply stating that a product or service is not intended for those under age 13 is unacceptable if reliable evidence regarding audience composition show a business's product or service is routinely accessed by a significant number of children under an age threshold.⁷¹ A business should be on constructive notice of its younger audience if, by using reasonable care or diligence, it becomes aware that minors are accessing their websites or services.⁷² Constructive knowledge could be established, for example, if a business receives credible data analytics that users include those aged 13-15, or if the business receives complaints from parents of children who indicate they are "pre-teens." In the alternative, if a business claims that it is unable to determine the age of its users with sufficient reliability, it should be required to default to the highest level of privacy protections.

Reasonable age-verification methods should also be proportional to the sensitivity of the personal information collected or used, or the content the child may be exposed to through the online service or product.⁷³ The more sensitive the personal information or harmful content involved, the higher degree of age certainty should be required. Importantly, children or parents should never provide more personal information than necessary to establish a user's age, or use that personal information for any other purpose than verification.

⁶⁹ Snow, *Why Age Verification Is So Difficult for Websites*, WSJ (Feb. 27, 2022) <<https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728>>.

⁷⁰ Ibid.

⁷¹ The FTC has previously encountered examples of such reliable evidence in the COPPA context. See, e.g., Compl. at par. 28, *U.S. v. Musical.Ly* (C.D. Cal., 2019, No. 2:19-cv-1439) (FTC alleged that receiving parental complaints about underage children using platform and prevalent child profile pictures and ages was sufficient to establish actual knowledge under COPPA that the business was collecting data from children).

⁷² A constructive knowledge rule standard would effectively counter excuses from businesses that are willfully ignorant of the true age composition of their audiences. See Fed. Trade Comm'n, *The Future of the COPPA Rule: An FTC Workshop*, pp. 61-62 (Oct. 7, 2019) <https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_par_t_1_1.pdf>.

⁷³ The UK ICO Children's Code adopts a robust age assurance provision as a standard of age appropriate design by requiring covered entities to: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead. UK ICO, *Age Appropriate Design: A Code of Practice for Online Services* (Sept. 2, 2020) <<https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>>.

To address these risks to children and the need for more stringent age verification procedures, the Commission could find that failure to implement appropriate age-verification procedures is an unfair business act or practice. One option for this regulation follows:

It is an unfair business act or practice for a business to provide an online service or product that it knows or should know is accessed by children without also implementing an age verification process that establishes a user's age with a level of certainty that is appropriate to the risk of potential harm that arises from the service or product. If the business cannot with reasonable accuracy determine the age of a user, it must, by default, set all privacy settings to their highest level of protection.

For purposes of age verification, a business shall generally avoid requesting additional information from the user. If, however, the business cannot verify the identity of the user from the information already maintained by the business, the business may request additional information from the user, which shall be used only for the purposes of verifying the age of the user. The business shall delete any personal information collected for the purposes of age verification as soon as practical after determining the user's age.

5. Businesses that collect and retain medical information must comply with reasonable data security standards.

Health data runs the gamut from seemingly innocuous, such as number of steps, to deeply sensitive, such as an untreatable cancer diagnosis. Although the Health Insurance Portability & Accountability Act (HIPAA) requires “Covered Entities”—typically providers of healthcare—and their “Business Associates” to preserve the confidentiality of health data and have procedures in place to protect it from unauthorized access or disclosure, the vast majority of websites and apps that collect health data from consumers may be outside of HIPAA’s reach.⁷⁴ In 2020, California brought an enforcement action against Glow, a fertility-tracking app that was designed to maintain deeply personal health information and had basic data security failures, because these security deficiencies violated state law requirements.⁷⁵ Despite having very sensitive and personal health information, Glow was not subject to HIPAA standards because it was not a “Covered Entity” as defined by HIPAA.

⁷⁴ Guidelines released by the U.S. Department of Health and Human Services indicate situations in which websites and apps must comply with HIPAA, and are narrowly limited to the circumstance in which the health care provider directly offers or contracts with the website or app. Dpt. of Health & Human Services, *Health App Use Scenarios & HIPAA* (Feb. 2016) <<https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf>>.

⁷⁵ Cal. Atty. Gen. Off., “Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women’s Personal and Medical Information” (Sept. 17, 2020) <<https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93>>; Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, Consumer Reports (July 28, 2016) <<https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/>>.

Glow was not alone in its lax security. One study evaluating 20,000 health apps found 23% of user data transmissions occurred on insecure channels, meaning they could be subject to eavesdropping and other data security breaches.⁷⁶ And without the specific legal compliance obligations of HIPAA, websites and apps can and do freely collect, store, analyze, and disclose personal health information. In the aforementioned study of 20,000 health apps, approximately 56% of the apps' data transmissions were to third parties, which a HIPAA-covered entity would not be able to do except in limited circumstances.⁷⁷ Additional studies also found popular period tracker apps with millions of downloads were sharing geolocation data and other personal information with numerous third parties involved in behavioral advertising and profiling, as well as failing to give clear guidelines on when and how much data could be shared with law enforcement.⁷⁸ Popular medical websites such as WebMD also share sensitive health data, including data related to the consumer's searches, with third-party trackers, who also receive information on which websites the consumer visits after navigating from the medical website.⁷⁹ Such information can be used to discriminate against, embarrass, or harass the consumer with targeted advertising or profiling, or put the consumer at risk for civil liability or criminal prosecution.⁸⁰ And in some cases, businesses that disclose personal health information can even present national security concerns, such as when the Strava fitness wearable device worn by servicemembers during exercise routines revealed the location of American military bases and patrol routes.⁸¹

⁷⁶ Tangari et al., *Mobile Health and Privacy: Cross-Sectional Study* (June 17, 2021) Brit. Med. J. 373:n1248 <<https://www.bmj.com/content/373/bmj.n1248>>.

⁷⁷ *Id.* See also Dpt. of Health & Human Services, *Summary of the HIPAA Privacy Rule* (Sept. 2022) <<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>> (summary of when HIPAA-covered entities may disclose medical information).

⁷⁸ ForbrukerRadet, *Out of Control: How Consumers are Exploited by the Online Advertising Industry* (Jan. 14, 2020) <<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>>; Mozilla Foundation, *In Post Roe v. Wade Era, Mozilla Labels 18 of 25 Popular Period and Pregnancy Tech with *Privacy Not Included Warning* (Aug. 17, 2022) <<https://foundation.mozilla.org/en/blog/in-post-roe-v-wade-era-mozilla-labels-18-of-25-popular-period-and-pregnancy-tracking-tech-with-privacy-not-included-warning/>>.

⁷⁹ Lefkowitz, *Study: Online Trackers Follow Health Site Visitors*, Cornell Chronicle (June 24, 2020) <<https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors>>.

⁸⁰ The risk of civil liability and criminal prosecution to pregnant people seeking abortions and those who assist them is especially high in light of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Org.* (2022) 597 U.S. __, __ [142 S.Ct. 2228, 2246]. Even before *Roe v. Wade* was overturned, law enforcement in Mississippi used a woman's search history to prosecute her for "killing her infant child" (the charges were eventually dropped). Parker, et al., *Texts, web searches about abortion have been used to prosecute women*, Wash. Post (Jul. 3, 2022) <<https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/>>. Law enforcement may also subpoena data from period-tracking or pregnancy apps to build their cases. *Id.*

⁸¹ Sly, *U.S. Soldiers are Revealing Sensitive and Dangerous Information by Jogging*, Wash. Post (Jan. 29, 2018) <https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html>.

Websites and apps not covered by HIPAA may have obligations under comparable state laws.⁸² But given the Commission’s jurisdictional authority, it should consider regulations that extend the same HIPAA privacy and security requirements to businesses that are not covered by HIPAA but collect and/or maintain equivalent health data, including but not limited to a consumer’s health history, condition, diagnosis, or treatment. Proposed language incorporating these principles could be:

It is an unfair business act or practice for any business that collects or maintains protected health information from a consumer to not have reasonable security appropriate to the sensitivity of the health information to protect the health information from unauthorized access, destruction, use, modification, or disclosure.

6. Health discrimination and disparities from algorithmic decision-making tools are inherently unfair and implicate the Commission’s regulatory authority regarding unfair business practices.

The ever-increasing, widespread use of artificial intelligence and algorithmic decision-making tools (AIA) in the healthcare industry raises serious concerns about fair and equitable access to quality healthcare for consumers—especially for those most at risk.⁸³ AIA may not be designed with affirmative animus or invidious intent, but may nonetheless contain bias.⁸⁴ The healthcare sector’s use of AIA remains a commercial area that would substantially benefit from additional regulation and guidance.⁸⁵

⁸² For example, California’s reasonable data security law and Confidentiality of Medical Information Act (CMIA) offer additional protections for health information that is held by businesses that would not qualify as Covered Entities or Business Associates under HIPAA. Like HIPAA, the CMIA applies to a provider of health care; unlike HIPAA though, the CMIA expands the entities considered providers of health care to businesses that offer software or hardware designed to maintain medical information. (Cal. Civ. Code, § 56.06, subds. (a), (b).)

⁸³ See Obermeyer et al., *Dissecting Racial Bias in an Algorithm used to Manage the Health of Populations* (Oct. 25, 2019) *Science* 336, 447-453; see also Begley, *Racial Bias Skews Algorithms Widely used to Guide Care from Heart Surgery to Birth, Study Finds*, *STAT* (June 17, 2020) <<https://www.statnews.com/2020/06/17/racial-bias-skews-algorithms-widely-used-to-guide-patient-care/>> (algorithms used by hospitals and physicians are “shot through with implicit racism ... which result in Black people receiving inferior care”); Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018) (negative biases about women of color are embedded in search engine results and algorithms).

⁸⁴ See Palmer, *‘It’s Not Going to Work’: Keeping Race Out of Machine Learning Isn’t Enough to Avoid Bias*, *STAT* (June 28, 2022) <<https://www.statnews.com/2022/06/28/health-algorithms-racial-bias-redacting/>> (citing research that algorithms based on clinical notes can predict patients’ self-identified race despite explicit redaction of race data).

⁸⁵ See Frakt, *Reagan, Deregulation and America’s Exceptional Rise in Health Care Costs*, *N.Y. Times* (June 4, 2018) <<https://www.nytimes.com/2018/06/04/upshot/reagan-deregulation-and-americas-exceptional-rise-in-health-care-costs.html>>; Moseley III, *History of Medicine The U.S. Health Care Non-System, 1908-2008* <<https://journalofethics.ama-assn.org/sites/journalofethics.ama-assn.org/files/2018->

The Commission's authority over unfair practices encompasses discrimination,⁸⁶ which can occur both intentionally and unintentionally and has resulted in widespread disparities and inequality in the healthcare industry.⁸⁷ While a history of explicit discrimination lies at the root of this inequity, it is often no longer driven by express animus.⁸⁸ Use of AIA occurs within the context of growing structural inequality, which directly correlates with poor health but is beyond the capacity of the healthcare industry to address on its own.⁸⁹ And although "data and

06/mhst1-0805.pdf>; Selbst & Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law* (forthcoming) 171 U.Penn. L.Rev. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4185227>.

⁸⁶ Jillson, *Aiming for Truth, Fairness, and Equity in your Company's use of AI*, Fed. Trade Comm'n (Apr. 21, 2021) <<https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>>.

⁸⁷ Roosli et al., *Bias at warp speed: how AI may contribute to the disparities gap in the time of COVID-19*, 28(1) *Journal of the American Medical Informatics Association*, 190-192 (2021); see also Villarosa, *Under the Skin: The Hidden Toll of Racism on American Lives and on the Health of Our Nation* (2022); McBride, *Caring For Equality: A History of African American Health and Healthcare* (2018) (history of African American struggle for medical and hospital care); Washington, *Medical Apartheid: The Dark History of Medical Experimentation on Black Americans from Colonial Times to the Present* (2006); Rothstein, *The Color of Law: A Forgotten History of How Our Government Segregated America* (2017).

⁸⁸ Sabin, *Tackling Implicit Bias in Healthcare* (July 14, 2022) *N.Engl. J. Med.* 387:2 <<https://www.nejm.org/doi/full/10.1056/NEJMp2201180>>; Majerol & Hughes, *CMS Innovation Center Tackles Implicit Bias*, *Health Affairs Forefront* (July 5, 2022) <<https://www.healthaffairs.org/doi/10.1377/forefront.20220630.238592>>; see also Bridges, *Implicit Bias and Racial Disparities in Health Care*, ABA <https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/the-state-of-healthcare-in-the-united-states/racial-disparities-in-health-care/>; Bridges, *Racial Disparities in Maternal Mortality* (Nov. 2020) 95 *N.Y. L.Rev.* 5; Bridges et al., *Introduction: Critical Race Theory and the Health Sciences* (2017) 43 *Am. J. Law & Med.* 179-182; Tong & Artiga, *Use of Race in Clinical Diagnosis and Decision Making: Overview and Implications*, Kaiser Family Foundation (Dec. 9, 2021) <<https://www.kff.org/racial-equity-and-health-policy/issue-brief/use-of-race-in-clinical-diagnosis-and-decision-making-overview-and-implications/>>; Burris et al., *Integrating Law and Social Epidemiology*, *Integrating Law and Social Epidemiology*, 30 *J. Law, Med. and Ethics* 510 (2002) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1004746> (discussing evidence regarding structural factors as the predominant influences on health); Matthews, *Just medicine: A Cure for Racial Inequality in American Health* (2015).

⁸⁹ Matthew, *Structural Inequality: The Real COVID-19 Threat to America's Health and How Strengthening the Affordable Care Act Can Help* (2020) 108 *Georg. L.J.* 1679, 1686-1688 <https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2020/06/Matthew_Structural-Inequality-The-Real-COVID-19-Threat-to-America%E2%80%99s-Health-and-How-Strengthening-the-Affordable-Care-Act-Can-Help.pdf>; Yearby, *Racial Disparities in Health Status and Access to Healthcare: the Continuation of Inequality in the United States due to Structural Racism* (2018) *Amer. J. of Econ. and Sociology* 77 (3-4), 1113-1152; Villarosa, *Under the Skin: The Hidden Toll of Racism on American Lives and On the Health of Our Nation* (2022) (discussing social determinants of health and the consequences of racial health inequality

algorithms risk reproducing biases against historically disadvantaged populations in ways that ‘look a lot like discrimination,’” current efforts to mitigate these harms must not be limited to antidiscrimination law, but should also be viewed as unfair practices.⁹⁰ Indeed, some commenters have noted that “any model developed in healthcare will be biased, because the data itself is biased; and how people access and interact with health systems in the U.S. is fundamentally unequal.”⁹¹ Concerns about the unfairness of AIA healthcare technology are compounded by the lack of transparency, and often even a lack of understanding—including by those who design and use them—of how such tools reach decisions and the empirical basis for them.⁹²

The Commission’s authority includes unfair practices that involve not only intentional discrimination, but also disparate treatment and harms resulting from systemic and structural determinants.⁹³ In grounding regulations in this authority, the Commission should be cognizant

combined with medical ignorance and discrimination); Kent, *How Social Determinants Data Can Enhance Machine Learning Tools*, Health IT Analytics (Oct. 28, 2020) <<https://healthitanalytics.com/news/how-social-determinants-data-can-enhance-machine-learning-tools>>.

⁹⁰ Hoffman, *Where Fairness Fails: Data Algorithms, and the Limits of Antidiscrimination Discourse* (2019) 22:7 Information, Communication and Society 900-915 <<https://www.tandfonline.com/toc/rics20/22/7>>; see also Gangadharan & Niklas, *Decentering Technology in Discourse on Discrimination* (2019) 22 Information Communication & Society 7, 882-899; Hayes & Schellenberg, *Discrimination is Unfair: Interpreting UDA(A)P to Prohibit Discrimination* (Apr. 2021) Student Borrower Protection Center Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3832022>.

⁹¹ Reuter, *In Scramble to Respond to Covid-19, Hospitals Turned to Models with High Risk of Bias*, Med City News (Apr. 21, 2021) <<https://medcitynews.com/2021/04/in-scramble-to-respond-to-covid-19-hospitals-turned-to-models-with-high-risk-of-bias/?rf=1>>.

⁹² Cabreros et al., *Predicting Race and Ethnicity To Ensure Equitable Algorithms For Health Care Decision Making* (Aug. 2022) Health Affairs 41, No. 8, 1153-1159; see also Shar & El-Sayed, *Medical Algorithms Need Better Regulation: Many do not require FDA approval, and those that do often do not undergo clinical trials* (Oct. 7, 2021) Scientific American <<https://www.scientificamerican.com/article/the-fda-should-better-regulate-medical-algorithms/>>.

⁹³ See Matthew, *Structural Inequality: The Real COVID-19 Threat to America’s Health and How Strengthening the Affordable Care Act Can Help* (2020) 108 Georg. L.J. 1679, 1705 (“[T]he health data reveal that the absence of legal equality and other documented unfair practices is a proximate cause of health disparities by race and ethnicity in America” and urging “lawmakers [to] join healthcare providers to realize this plain meaning of equality”); Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and A Path Forward for the Federal Trade Commission* (2021) Y.J. Law & Tech. 1, 42-43 (“That it has limitations does not mean, however, that the FTC’s unfairness authority cannot be used to combat the fundamentally unfair phenomenon of unlawful discrimination, as well as ... other algorithmic harms.”); Barocas & Selbst, *Big Data’s Disparate Impact* (2016) 104 Calif. L. Rev. 671 (discussing the necessity to reexamine the meanings of “discrimination” and “fairness”); Selbst & Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law* (forthcoming) 171 U.Penn. L.Rev.; Hoffman, *Where Fairness Fails: Data Algorithms, and the Limits of Antidiscrimination Discourse* (2019) 22:7 Information, Communication and Society 900-915 <<https://www.tandfonline.com/toc/rics20/22/7>>; Suddath, *A Very Dangerous Place to Be Pregnant Is Getting Even Scarier: Texas leads the US in maternity ward closures, and nowhere is this*

that gathering and using demographic data, including racial or ethnic variables, is not in itself evidence of discrimination, and in fact may be crucial to identify, evaluate, and address health disparities.⁹⁴ Healthcare entities may use these variables as part of a proactive effort to ensure equity and ameliorate effects of past discrimination in healthcare.⁹⁵ The Commission should make clear in any regulations that it does not intend to interfere with such efforts.

In light of the above, and based on California's own, on-going efforts in this area,⁹⁶ we offer the following guiding principles, as opposed to specific regulatory language, for consideration in drafting regulations related to the use of AIA:

- *A business commits an unfair business act or practice if it uses artificial intelligence or other automated decision-making tools in such a way as to have a disproportionate, adverse impact on or causes disproportionate, adverse treatment of a consumer or a class of consumers on the basis of protected characteristics.*
- *It can be an unfair business act or practice for a developer to sell or a business to utilize AIA without testing, auditing, monitoring, disclosures, and transparency. Transparency measures could include disseminating data and source code for independent review and testing, and disseminating the results of internal and independent audits. It is an unfair business act for an entity to refuse transparency, audit, or monitoring measures.*

more of an issue than in the western part of the state, Bloomberg (Aug. 4, 2022)

<<https://www.bloomberg.com/news/features/2022-08-04/texas-pregnancy-care-worsens-as-maternity-wards-close#xj4y7vzkg>>.

⁹⁴ See e.g., National Academy for State Health Policy, *Achieving Progress Toward Health Equity Using Race and Ethnicity Data: State Strategies and Lessons Learned* (Nov. 15, 2021)

<<https://www.nashp.org/achieving-progress-toward-health-equity-using-race-and-ethnicity-data-state-strategies-and-lessons-learned/>>; Commonwealth Fund, *Improving Race and Ethnicity Data Collection: A*

First Step to Furthering Health Equity Through the State-Based Marketplace (2022)

<<https://www.commonwealthfund.org/blog>>.

⁹⁵ See, e.g., Samorani et al., *Overbooked and Overlooked: Machine Learning and Racial Bias in Medical Appointment Scheduling* (Aug. 18, 2021) Manufacturing & Service Operations Management

(describing “race aware” changes to algorithm to alleviate waiting room times for Black patients who were otherwise more likely to be overbooked); Penman-Aguilar, *Measurement of Health Disparities, Health Inequities, and Social Determinants of Health to Support the Advancement of Health Equity*, J. Public Health Manag. Pract. (2016) 22(Suppl. 1): S33–S42

<<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5845853/>>; Weber & Pepin, *Why Law Is a Determinant of Health* (2021) 50 Stetson L.Rev. 401; Horton, *The rule of law—an invisible determinant of health* (2016) 387 The Lancet 1260.

⁹⁶ My office is currently investigating racial and ethnic bias in algorithmic decision making in healthcare. See Letter from California Attorney General Rob Bonta to Hospital CEOs (Aug. 31 2022)

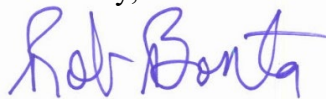
<<https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare>>.

- *Health care entities' attempts to address and ameliorate disparities based on race or other protected characteristics are not per se unfair.*
- *Fairness-based consumer protection regulations should mandate evaluation of the potential disparate health impacts and consequences of industry practices and products, particularly on historically disadvantaged protected classes and other vulnerable populations—including those currently not legally recognized as protected from discrimination (e.g., the unhoused, those living in remote rural areas, and other populations grappling with barriers to healthcare). This evaluation should occur prior to a product or tool entering the marketplace.*

Conclusion

Preventing unwanted commercial surveillance is a necessary first step towards protecting consumers' privacy and personal information. Businesses should be incorporating privacy from day one, and integrate privacy-by-design at every critical point of development. To effectuate a stronger national privacy framework grounded in the FTC's existing authority, the Commission should embrace this opportunity to establish obvious necessary baseline requirements that protect and advance consumer privacy.⁹⁷ This will protect consumers, provide clarity to businesses, and fortify our democracy. Thank you for the opportunity to share California's enforcement experience and provide this public comment.

Sincerely,



ROB BONTA
Attorney General

⁹⁷ I further commend the Commission's recent policy statement on unfair competition. See Fed. Trade Comm'n, Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act, Commission File No. P221202 (Nov. 10, 2022) <<https://www.ftc.gov/legal-library/browse/policy-statement-regarding-scope-unfair-methods-competition-under-section-5-federal-trade-commission>>.