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

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 request[2] 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 title[3] 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 advertising[5]—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.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS&sectionNum=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 Brodkin, *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 hurts 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.