March 8, 2019

California Department of Justice
300 S. Spring Street
Los Angeles, CA 90013
ATTN: Privacy Regulations Coordinator

Re: Rules Implementing the California Consumer Privacy Act (CCPA)

Consumer Reports[1] appreciates the opportunity to submit input to the California Attorney General's office (AG) as it prepares to propose rules to implement the California Consumer Privacy Act (CCPA). Consumer Reports has long fought to expand privacy protections for consumers, and is pleased that the CCPA guarantees important privacy safeguards, including the right to opt-out of the sale of personal information.[2] The AG has the opportunity to ensure that the CCPA is workable for consumers, as it has broad leeway to issue regulations to further the privacy intent of the CCPA.[3] The AG should issue common-sense proposed rules that would:

- Maintain the definition of personal information;
- Tighten restrictions on targeted advertising;
- Restrict access and deletion rights with respect to unauthenticated data;
- Make it easy to opt-out of the sale of personal information, by requiring companies to honor Do Not Track signals and by creating a Do Not Sell registry modeled after the National Do Not Call Registry;
- Put reasonable limits on financial incentives for the sharing or sale of personal information to third parties; and
- Require detailed privacy policies that provide real transparency and impose limits on companies' data practices.

Now, more than ever, consumers want real privacy protections. Currently, the burden is on the consumer to decipher long, confusing privacy policies, or to decide between using a potentially helpful service or device and guarding their privacy. And, they're fed up. 92 percent of Americans think that their Internet Service Provider (ISP) should obtain their permission before sharing their data with third parties.[4] Over

[1] 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.
[2] Sec. 1798.120
[3] Sec. 1798.185
[4] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, CONSUMER REPORTS (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data/.

Headquarters Office
101 Truman Avenue
Yonkers, New York 10703-1057
(914) 378-2029

South West Office
11801 Domain Blvd, 3rd Floor
Austin, TX 78701
(512) 477-4431

Washington Office
1101 17th Street, NW #500
Washington, DC 20036
(202) 462-6262

West Coast Office
1535 Mission Street
San Francisco, CA 94103-2512
(415) 431-6747

half don't trust social media companies to keep their information safely protected.[5] And almost three-quarters said that it's very important to have control over their information.[6] Recent scandals involving the illicit sharing or sale of personal information without consent, such as the Cambridge-Analytica incident[7] and reports of unauthorized location tracking,[8] have revealed broad unease among the general public of data sharing without the consumers' active consent. Clearly, consumers value their devices, connected products, and other apps and services, but they don't have the confidence that their information is safe. Consumers and businesses need clear rules of the road with protections that ensure that consumers have privacy by default.

1. The AG should reject requests to narrow the categories of personal information covered by the law and the definition of unique identifier, to ensure that sensitive data is protected.

The CCPA gives the AG the authority to adjust the categories of personal information covered by the legislation, as well as the definition of unique identifier, in order to reflect "changes in technology, data collection, obstacles to implementation, and privacy concerns."[9] 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.[10] The AG should reject requests to narrow information covered by the CCPA, which would eliminate important rights for consumers and directly counter legislative intent.

While there are valid concerns about access and deletion rights to device- and household-level information in shared environments—members of a household should not be allowed to access unauthenticated data because they could end up accessing the private information of another person—those concerns should be dealt with narrowly, for example, by restricting access and deletion rights to unauthenticated data (see *infra*, section 3). With respect to information tied to a device, if the device has a discrete and known number of users, it may be appropriate to provide access and deletion if practicable to get consent from all users.[11] It should not be dealt with by limiting the definition of personal information, which would remove consumers' ability to opt out of its sale—a key protection under the law. Bill sponsor Alastair MacTaggart laid out an expansive definition of personal information, which includes information that is "capable of being associated with . . . a particular consumer or household"[12] to cover the ways that companies use and share information today, including for advertising purposes.[13]

---

[5] Lee Rainie, *Americans' Complicated Feelings about Social media in an Era of Privacy Concerns*, PEW RESEARCH CTR. (Mar. 27, 2018) http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[6] Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[7] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[8] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, MOTHERBOARD (Jan. 8. 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[9] Sec. 1798.185(a)(1)-(2)

[10] 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 [hereinafter Chamber Letter].

[11] Electronic Frontier Foundation, EFF Comments to the California Attorney General Regarding CCPA Rulemaking at 4 (Mar. 8, 2019) [hereinafter EFF Comments].

[12] Sec. 1798.140(o)(1)

[13] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley — and Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

Device and household-level data is very sensitive, and consumers deserve protections around its use—particularly the right to opt out of its sale.

Removing IP address from the definition of personal information would weaken protections against the sale of location data to ad tech companies, data brokers, and other third parties. Many IP addresses are static or change infrequently, allowing companies to track user behavior over time even without access to cookies or other identifiers.[14] Moreover, correlation of IP addresses is one of the most effective 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.[15] Currently, the CCPA gives consumers the right to opt out of its sale to third parties, but removing IP address from the definition of personal information would rescind this right.

Covering household data is important as well. Household data—collected through services like Nest or communal devices such as smart TVs—can also be used to track whether consumers are in their home or not—a potential gold mine for thieves.[16] Facebook recently took out a patent to better determine the family members or others that consumers live with—by using facial recognition technology to analyze photos posted on Facebook or Instagram. This information would then be used to better target advertising towards consumers.[17] Again, consumers find this information to be extremely sensitive—85 percent consider relationship history to be sensitive information.[18] Thus, it would be inappropriate to narrow the definition of personal information.

On the other hand, we do not object to the AG clarifying that the phrase "capable of being associated"[19] in the CCPA's definition of personal information does not render *any* piece of information necessarily covered by CCPA. Rather, only information that could reasonably be associated with a person, device, or household should be considered within the scope of the law's protections.

2. The AG should tighten restrictions on targeted advertising.

Targeted advertising, including based on pseudonymous data, must remain covered by the legislation, and other collection methods such as social sharing widgets should fall under the scope of sale as well. While industry groups such as the California Chamber of Commerce have sought to explicitly exempt behavioral advertising from the CCPA's right to access and third-party sharing opt-out protections,[20] this undermines a main goal of the CCPA and ignores consumers' stated preferences. A principal purpose of the CCPA is to give consumers the ability to opt out of the sale of their personal information, including for online advertising. Bill sponsor Alastair MacTaggart sought to "slowly dry up the supply of personal information that companies could buy or trade on the open market" in order to address some of the worst abuses.[21] For example, while many state statutes cover only a handful of types of personal

[14] Dennis Hartman, *The Advantages & Disadvantages to a Static IP Address*, TECHWALLA (last visited March 7, 2019), https://www.techwalla.com/articles/the-advantages-disadvantages-to-a-static-ip-address.
[15] *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.
[16] Lauren Kirchner, *Your Smart Home Knows a Lot About You*, PROPUBLICA (Oct. 9. 2015), https://www.propublica.org/article/your-smart-home-knows-a-lot-about-you.
[17] Nicole Nguyen, *Facebook Filed a Patent to Predict Your Household's Demographics Based On Family Photos*, BUZZFEED NEWS (Nov. 16, 2019), https://www.buzzfeednews.com/article/nicolenguyen/facebook-household-prediction-patent
[18] Mary Madden, *Americans Consider Certain Kinds of Data to be More Sensitive than Others*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/.
[19] Sec. 1798.140(o)(1)
[20] Chamber Letter, *supra* note 10, at 10.
[21] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley — and Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

information,[22] the privacy provisions in the CCPA cover a broad swath of consumer data, including information tied to a device, to give consumers control over the data used for advertising purposes.[23] Similarly, the CCPA has an inclusive definition of the "sale" of information, to help ensure that consumers can opt out of data sharing for online advertising.[24] If a consumer who opts out of the sale of their data on an shoe store's website ends up seeing retargeted ads for those shoes all over the internet, consumer choice will be frustrated, and the CCPA will have failed to achieve its objectives.

Furthermore, the AG should clarify that all online sharing for measurement, analytics, and related uses should be considered within the scope of sale unless the recipient is prohibited from any beneficial secondary usage of the data. Cross-site, app, and service measurement and analytics data can be very sensitive. The CCPA places no limits on the ability of companies to collect data to advertise to their own customers. But, it enforces much-needed accountability in the context of the current ecosystem by placing real limits on companies all along the data-sharing chain and disincentivizing data purchases. If online tracking is considered outside of scope of the CCPA, then it would not achieve its stated goals. Data brokers were the intent of the bill,[25] and online ad tech companies—including Facebook and Google—are the modern data brokers. As Berkeley professor Chris Hoofnagle explains, Google and Facebook provide app developers privileged, valuable information—your data—in return for services that help increase engagement with their platforms.[26]

For that same reason, it's important to tighten operational exceptions for consumers' opt-out choices. Section 1798.140(t)(2)(C) states that the business purpose exemption for service providers is allowed only when *necessary* for those purposes. However, this exception must not be allowed to swallow the rule, allowing for profligate third-party sharing contrary to user directives and expectations. Last year, Facebook made headlines when they were discovered to have given companies like Microsoft, Amazon, and Spotify extensive access to consumer data under the guise of a "service provider" relationship.[27] Recently, Mark Zuckerberg published an op-ed in the *Wall Street Journal* that implied that millions of websites and apps needed to share details of website visits with Facebook for security and account fraud prevention.[28] The AG should clarify that sharing in spite of an opt-out instruction must be reasonably constrained and proportionate, and subject to reasonable retention requirements. The Electronic Frontier Foundation articulated a set of rules for limited operational sharing despite receiving a browser "Do Not Track" instruction; that guidance should inform the AG's own guidance around reasonable exceptions.[29]

3. The AG should restrict access and deletion rights with respect to unauthenticated data to ensure that consumer privacy is protected.

The CCPA also empowers the AG to establish rules regarding requests to access and delete personal information—including honoring those submitted by a consumer logged into an account with the company and those without an online account.[30] <u>While we strongly urge the AG to maintain an</u>

---

[22] See, for example, California's data breach notification statute, California Civil Code 1798.82.
[23] Sec. 1798.140(o)(1)(A)
[24] Sec. 1798.140(t)(1)
[25] Confessore, *supra* note 21.
[26] Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.
[27] 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/2018/12/18/technology/facebook-privacy.html.
[28] Mark Zuckerberg, *The Facts About Facebook*, WALL ST. J. (Jan. 24, 2019), https://www.wsj.com/articles/the-facts-about-facebook-11548374613.
[29] Electronic Frontier Foundation, A Privacy-Friendly Do Not Track (DNT) Policy (last visited March 7, 2019), https://www.eff.org/dnt-policy.
[30] Sec. 1798.185(a)(7)

expansive definition of personal information, including information associated with a device and a household, the AG should clarify that unauthenticated data is exempt from access and deletion rights.

To avoid unauthorized and inappropriate disclosure of personal data in responding to requests, steps must be taken to verify identity, for both consumers that have an online account with a company and those that do not. Even consumers who have logged in to their accounts should be required to log-in separately for access and deletion requests, to help avoid unauthorized access to their personal information.[31] Additionally, the use of two-factor authentication should be encouraged.[32] Consumers without online accounts with the company should be required to provide additional identification to prove that they are the person whose information has been collected and used.[33] For third-party access requests, the third party must prove that they have the authorization of the consumer to submit access and deletion requests.[34]

The AG should allow companies to deny access and deletion requests when the data cannot be authenticated or reasonably tied to a specific person. While transparency, data portability, and access rights are incredibly important, the risk of disclosure of sensitive information to a person other than the consumer is simply too great. In addition, while the CCPA already notes that businesses need not reidentify or link data in order to comply with access requests,[35] we have no objection to clarifying further that there is no need to collect and associate information with a real name in order to provide access.[36] Otherwise, there is the potential that someone other than the consumer, including a spouse or roommate, could obtain sensitive information about the consumer without their authorization.

Companies that can tie specific data to an individual *must* provide the specific pieces of information as mandated by CCPA. For example, companies often supplement their files with information from data brokers.[37] It's important for accountability that consumers are able to access those specific pieces of data. Some limitations on access may be appropriate. For example, we have no objection to clarifying that companies are not required to release financial account information, birthdates, or SSNs or other specific pieces of information that could be used for identity theft.[38]

4. The AG should make it easy to opt-out of the sale of personal information, by requiring companies to honor Do Not Track signals and by creating a Do Not Sell registry modeled after the National Do Not Call Registry.

An opt-out regime can only work if consumers can opt out universally with simple tools. Opting out site by site, store by store is not practical. To remedy this, the AG should (1) clarify that companies need to comply with platform-level opt-outs similar to IoS Limit Ad Tracking and Do Not Track if offered. The AG should also (2) set up a registry of identifiers, such as email addresses, phone number, etc., for users to globally opt out of the sale of their information.

Companies should be required to honor global, platform-level requests to opt out of the sale of consumer data. Currently, browsers including Internet Explorer[39] and Chrome[40] give consumers the option to

[31] EFF Comments, *supra* note 11, at 3.
[32] *Id*.
[33] *Id*. at 4.
[34] *Id.* at 5.
[35] Sec. 1798.110(d)(2)
[36] Chamber Letter, *supra* note 10, at 8.
[37] *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N at 24 (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[38] Chamber Letter, *supra* note 10, at 8. In these instances, companies should still be required to disclose the category of information collected.
[39] Microsoft, Use Do Not Track in Internet Explorer 11 (last visited March 7, 2019),

indicate their tracking preferences. Do Not Track signals from a California IP address could be interpreted as an opt out, or browsers could offer new signals to publishers to convey CCPA opt-out requests to all publishers.[41] Selecting these platform controls clearly indicates that a consumer intends to limit the sharing of personal information to third parties. For unauthenticated data not associated with a specific person, platform-level controls are the most efficient manner to globally convey opt-out requests.

Second, the AG should create and house a Do Not Sell registry, modeled on the FTC's popular Do Not Call (DNC) registry, that businesses would be required to check before selling consumer data tied to those identifiers. The AG would collect consumers' identifiers, such as emails and phone numbers, and companies would pay in order to consult the list (thus ensuring that companies seeking to sell data would absorb the costs for the operation of the website). Consumers could add their identifiers to the registry through public portal, much like Do Not Call. This would enable consumers to easily and globally express their preferences to opt-out of the sale of their data. Companies should be required to check this database before selling (or purchasing) consumers' information, much as they do today for the DNC registry. The DNC registry currently includes over 235 million numbers, indicating that this is an easy way for consumers to opt out of telemarketing messages.[42] The same should be done for online privacy. Sen. Ron Wyden, in his proposed Consumer Data Protection Act, outlines a similar system to facilitate global opt outs for both unauthenticated and authenticated data.[43]

Finally, we have no objection to the AG clarifying that business may offer consumers the opportunity to opt out of the sale of some, but not all, of their data,[44] as long as companies are also required to provide a way to opt out of all third party sales at once under the CCPA. Companies should make it as easy as possible for consumers to opt-out of the sale of their data by giving them a universal opt-out, but the CCPA does not prohibit, and we have no objection to, businesses creating multiple options for consumers.

5. With respect to financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack adequate choices.

The existing text of the CCPA supports loyalty programs that reward consumers for repeated patronage. A loyalty program rewards customers for what they buy (e.g., every tenth coffee is free). Businesses collect consumer data in order to determine those rewards. The CCPA does not address or regulate this type of collection of data at all—leaving businesses free to create these programs. As such, we have no objection to the AG clarifying further that legitimate loyalty programs are permitted under the CCPA.[45] However, the AG should exercise its rulemaking authority with respect to financial incentives programs to clarify that discriminatory treatment should be presumed where markets are consolidated.

---

https://support.microsoft.com/en-ca/help/17288/windows-internet-explorer-11-use-do-not-track.

[40] Google Chrome Help, Turn "Do Not Track" On or Off (last visited March 7, 2019), https://support.google.com/chrome/answer/2790761?co=GENIE.Platform%3DDesktop&hl=en.

[41] Electronic Frontier Foundation, Do Not Track (last visited Dec. 18, 2018), https://www.eff.org/issues/do-not-track.

[42] *National Do Not Call Registry Data Book FY 2018*, Federal Trade Commission at 5 (Nov. 2018), https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2018/2018_dnc_data_book_0.pdf. The efficacy of the DNC registry is of course limited by the fact that it only applies to legitimate telemarketers, and that it does not hinder scammers, debt collectors, and others in their communications.

[43] Consumer Data Protection Act, Discussion Draft (2018), https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf.

[44] ANA Urges California Attorney General to Clarify Key Provisions of California Consumer Privacy Act (CCPA) (Jan. 14, 2019), https://www.ana.net/content/show/id/52341 [hereinafter ANA Letter].

[45] *Id.*

Loyalty programs are clearly permitted under the CCPA. The CCPA provides a wide exemption in the right to delete provision in order "to provide a good or service requested by the consumer."[46] This certainly accommodates rewards programs. The *fundamental purpose* of a loyalty program is to track purchases in order to determine when a customer is entitled to a free or discounted good. For example, someone who signs up for a coffee shop rewards program is requesting that the company log how many coffees she has purchased. This type of user-requested information collection is clearly allowed under the CCPA. Of course, the customer may have a right to delete *other* data that the company maintains, and of course can decide not to participate in the loyalty program at all.

Unfortunately, the CCPA goes even further to allow companies to offer financial incentives for the sale of personal information to third parties. True loyalty programs simply keep track of customer purchasing in order to incentivize repeat business. But other, more exploitative programs could provide discounts in exchange for building a profile for targeting offers, or could sell information about customer habits to third-party data brokers. The CCPA explicitly states that companies can charge higher prices to consumers who limit access to their data and can offer financial incentives to consumers for the collection and sale of their personal information.[47] This language was added to the CCPA over objections from advocates, who argued that consumers should not be penalized for exercising their privacy rights.[48] That behavior does nothing to reward consumer loyalty, and runs counter to what participating consumers would reasonably expect. For this reason, the California Supermarket Club Disclosure Act of 1999 already puts important limits on many California retailers—those that sell food—with respect to these exploitative practices.[49]

Discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The AG currently has the authority under the CCPA to issue rules prohibiting the use of financial incentives in market sectors that lack competition,[50] and we urge the AG to do so. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates—about $30 per month—for not leveraging U-Verse data for ad targeting.[51] Where consumers have few choices, market forces don't impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,[52] further highlighted by the creation of a new Federal Trade Commission task force to monitor these trends.[53] The AG should exercise its authority to put reasonable limits on the these programs in consolidated markets.

6. The AG should require detailed privacy policies that provide real transparency and impose limits on companies' data practices.

---

[46] Sec. 1798.105(d)(1)
[47] Sec. 125(a)(2) and 125(b)
[48] 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.
[49] California Civil Code 1749.60
[50] Sec. 1798.125(b)(4)
[51] 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/.
[52] *Too Much of a Good Thing*, ECONOMIST (March 26, 2016), https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing.
[53] *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.

Consumers dislike reading privacy policies,[54] but they serve a real purpose. The FTC typically takes action against companies for privacy reasons only when they violate their terms of service.[55] Because there are no requirements for these disclosures, and because most FTC privacy cases are predicated upon a specific misstatement in a privacy policy or elsewhere, companies tend to make privacy policies as expansive as possible, so as to shield themselves from lawsuits and other enforcement actions.[56] To address this problem, privacy policies must provide detailed information about practices. The primary audience is not consumers but regulators, the press, and testing organizations like Consumer Reports.

These documents should be used primarily as compliance and accountability tools—so that intermediaries can hold companies accountable for the standards set forth in these documents. The AG 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. The AG should supplement these mandatory, detailed disclosures with requirements to first provide simple instructions for consumers seeking to take advantage of their privacy rights. These bifurcated privacy policies would prioritize the actionable information for consumers while also providing substantially more information for those few with the bandwidth and interest to process such information.

Finally, we have no objection to the AG issuing guidance that companies need not develop individualized privacy policies containing specific pieces of personal information collected about the consumer. In the hearings and in written testimony, some industry representatives have raised concerns that the requirement in 1798.110(c) for companies to provide to consumers disclosures about the specific pieces of personal information the business has collected about that consumers could be interpreted to mean that each company must create an individualized privacy policy for consumers.[57] As explained by sponsors Alastair MacTaggart and Common Sense Media, that is not the drafters' intent.[58] We agree that companies should not be required to create individualized privacy policies for each consumer, and we have no objection to the AG issuing guidance to that effect.

Conclusion

Thank you for accepting feedback on the implementation of the CCPA. We look forward to continuing to work with you throughout the rulemaking process.

Justin Brookman
Director, Consumer Privacy and Technology Policy
Washington, DC

Maureen Mahoney
Policy Analyst
San Francisco, CA

---

[54] 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.
[55] *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.
[56] Id. at 19.
[57] ANA Letter, *supra* note 44.
[58] Californians for Consumer Privacy and Common Sense Kids Action, Recommended Technical Amendments to AB 375 & SB 1121 (Jan. 19, 2019), https://www.caprivacy.org/post/recommended-technical-amendments-to-ab-375.