February 25, 2020

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

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

Consumer Reports[1] thanks the California Attorney General's office (AG) for the opportunity to comment on its proposed changes to rules implementing the California Consumer Privacy Act (CCPA).[2] The landmark CCPA gives California consumers, for the first time, the ability to access, delete, and stop the sale of their personal information. Californians finally have a real opportunity to exercise their constitutional right to privacy. But tech companies have been able to avoid meaningful regulations for decades, and their behavior suggests that they're not going to let the CCPA get in the way of their sale of consumers' personal information.

It's up to the AG to hold companies accountable, especially as many of them have willfully ignored the CCPA since it went into effect in January.[3] Making matters worse, several of the changes to the draft rules proposed by the AG take a significant step back from the draft released in October. Most concerning, the updated rules exempt IP addresses from the definition of personal information—an unacceptable change that would dramatically weaken the existing statute. To protect consumers, we urge the AG to:

[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. Consumers Reports works for pro-consumer policies in the areas of financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, telecommunications and technology, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace. 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] California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Feb. 10, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf [hereinafter CCPA Modified Regulations].

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

- **Clarify that sharing for cross-context targeted advertising falls under the definition of sale;**
- **Tighten the service provider exemption;**
- **Remove the new limits on the definition of personal information, which would create a significant loophole for targeted advertising;**
- **Make global, browser opt-outs more user-friendly;**
- **Clarify that financial incentives in markets that lack competition is an unfair and usurious practice;**
- **Require companies to forward opt-out requests to third-party recipients of data where possible; and**
- **Consider a retention limit on records of deletion.**

More information continues to become known about the extent to which consumers' personal information—collected not only online, but through their phone handsets, apps, televisions, and smart devices—is bought and sold without their knowledge,[4] and the lengths to which companies will go to avoid complying with even baseline privacy protections. The AG needs to take swift action to ensure that consumers are able to exercise their privacy rights.

The AG should clarify that sharing for cross-context targeted advertising falls under the definition of sale.

Many tech companies are doing everything they can to avoid complying with consumer's explicit requests to opt-out of the sale of their information. Even though companies had ample time to prepare to comply with the new law, they are now actively looking for loopholes, and some are ignoring the CCPA altogether. For example, the Interactive Advertising Bureau (IAB), a trade group that represents the ad tech industry, developed a framework for companies to evade the opt-out by abusing a provision in the CCPA meant to permit a company to perform certain limited services on its behalf.[5] Google announced that it will follow IAB's lead,[6] and Facebook has announced that its "like" buttons, which allow the company to track users' behavior across the web—even if they are not logged in—is outside of the consumer opt-out clause.[7] Grindr, for

[4] *Out of Control: How Consumers Are Exploited by the Online Advertising Industry*, NORWEGIAN CONSUMERS COUNCIL (Jan. 14, 2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf [hereinafter OUT OF CONTROL].

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

[6] Allison Schiff, *Google Will Integrate With IAB Tech Lab's CCPA Compliance Specs By Jan. 1 Deadline*, ADEXCHANGER (Dec. 4, 2020), https://www.adexchanger.com/privacy/google-will-integrate-with-iab-tech-labs-ccpa-compliance-specs-by-jan-1-deadline/; Google, Helping Advertisers Comply with CCPA in Google Ads (last visited Feb. 23, 2020), https://support.google.com/google-ads/answer/9614122.

[7] Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345 [hereinafter *Facebook Won't Change Web Tracking*].

example, seeks to ignore "do not sell" instructions by claiming that consumers have assented to sale in long-form contracts they almost certainly have never read.[8]

The AG has the opportunity to provide further clarity on this issue, much of which hinges on the definition of sale and the regulations around service providers. With respect to sale, some incorrectly claim that because money isn't necessarily exchanged for data, then data transfers for targeted advertising purposes aren't a sale—therefore, consumers don't have the right to opt-out.[9] For example, retailers may send adtech platforms both money and data collected about consumers to target ads on multiple sites. But addressing targeted advertising is one of the main goals of the CCPA, which has an inclusive definition of personal information and a broad definition of sale to cover transfers of data for these purposes.[10]

To help address any potential loopholes, the AG should exercise its broad authority to issue rules to further the privacy intent of the Act,[11] and clarify that the transfer of data between unrelated companies for any commercial purpose falls under the definition of sale. This will help ensure that consumers can opt-out of cross-context targeted advertising. We suggest adding a new definition to § 999.301:

> "Sale" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

While we appreciate that the AG has attempted to address instances of non-compliance with the opt-out button requirement by adding a provision to limit companies to "minimal steps to allow the consumer to opt-out[,]"[12] that won't be enough to stop these companies. It is true that one of the characteristics of IAB's framework for "compliance" with the CCPA is that consumers are directed to multiple sites to opt-out (IAB purports to send consumers to existing failed self-regulatory mechanisms to exercise choices about targeted advertising).[13] But the fundamental problem is that companies argue that most commercial data transfers aren't a sale, so that they

---

[8] Natasha Singer and Aaron Krolik, *Grindr and OkCupid Spread Personal Details, Study Says*, N.Y. TIMES (Jan. 13, 2020), https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html.

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

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

[11] Cal. Civ. Code § 1798.185(a).

[12] CCPA Modified Regulations, *supra* note 2, at § 999.315.

[13] *IAB Framework*, *supra* note 5, at (III)(2)(d)(ii).

don't have to put up the opt-out button or comply with consumer requests. This issue needs to be decisively addressed.

The AG should tighten the service provider exemption to stop inappropriate data sharing in spite of an opt-out.

To address a second loophole that the IAB has exploited, the AG should clarify that when the consumer has opted out of the sale of their information, data cannot be shared—even with a service provider—to target advertising on another site or service. The AG's new § 999.314(d), stating that "A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business" is an improvement on the previous draft rules, which were silent on the issue. Nevertheless, the language should be tightened, especially since some incorrectly claim that the data-sharing engaged in for targeted advertising purposes is not a sale.[14] We suggest a new § 999.314(d):

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

Second, the AG should take action to stop companies from combining data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they're just service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets. To help address this problem, the AG has appropriately removed language in § 999.314(c) of the previous draft, which held that service providers can merge data across clients. But in the absence of a specific prohibition, given its disregard for the FTC consent order, Facebook (and other companies) will likely continue to engage in this behavior. The AG needs to make clear that this is not acceptable. We suggest the following language:

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

[14] *IAB Framework*, *supra* note 5, at (II)(3).

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.[15] The AG should refine the draft regulations in order to give consumers more control over their data with respect to these practices.

A history of non-compliance

Consumers who dislike ad tracking and targeted advertising will be frustrated if sending CCPA "Do Not Sell" instructions has no practical effect. Consumers in Europe have already experienced this following widespread noncompliance with GDPR as websites force consumers through coercive consent dialogs to justify perpetuating existing data practices.[16] Complaints about tracking abuses have been filed with European regulators.[17] And the Information Commissioner's Office (ICO), which is the UK GDPR regulator, has declared industry real-time bidding (RTB) behaviors—when publishers auction off a space to advertisers, based on your past internet activity, in a fraction of a second—to be violative of GDPR.[18] So far, regulators have yet to take real enforcement action.[19] The AG shouldn't make the same mistake that European regulators have made.

Ad tech companies have a long history of evading regulation. In 2012, industry representatives committed to honoring Do Not Track instructions at a White House privacy event.[20] Over the next few years, however, as regulatory pressure and the prospect of new legislation faded, industry backed away from its commitment, with trade groups publicly announcing withdrawal from the industry standard process at the World Wide Web Consortium.[21] Instead, they set up

---

[15] 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.
[16] Kate Fazzini, *Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, but So Far It's Mostly Created Frustration for Users, Companies, and Regulators*, CNBC (May 5, 2019), https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html.
[17] Steven Melendez, *How Google Is Breaking EU Privacy Law, According to a New Complaint*, FAST COMPANY (Sept. 13, 2018), (https://www.fastcompany.com/90236273/google-faces-gdpr-privacy-complaint-over-its-targeted-ads-from-brave-browser; Natasha Lomas, *Google and IAB Ad Category Lists Show 'Massive Leakage of Highly Intimate Data,' GDPR Complaint Claims* (Jan. 27, 2019), TECHCRUNCH, https://techcrunch.com/2019/01/27/google-and-iab-ad-category-lists-show-massive-leakage-of-highly-intimate-data-gdpr-complaint-claims/.
[18] Update Report Into Adtech and Real Time Bidding, INFORMATION COMMISSIONER'S OFFICE (Jun. 20, 2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[19] Simon McDougall, *Blog: Adtech - The Reform of Real Time Bidding Has Started and Will Continue*, ICO (Jan. 17, 2020), https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.
[20] Dawn Chmieleski, *How 'Do Not Track' Ended Up Going Nowhere*, RECODE (Jan. 4, 2016), https://www.vox.com/2016/1/4/11588418/how-do-not-track-ended-up-going-nowhere; *see* Julia Angwin, *Web Firms to Adopt 'No Track' Button*, WALL ST. J. (Feb. 23, 2012), https://www.wsj.com/articles/SB10001424052970203960804577239774264364692.
[21] Kate Kaye, *Do-Not-Track on The Ropes as Ad Industry Ditches W3C*, ADAGE (Sept. 17, 2013), http://adage.com/article/privacy-and-regulation/ad-industry-ditches-track-group/244200/.

their own voluntary "Ad Choices" system to allow consumers to opt-out of interest-based advertising. But industry efforts to self-regulate have largely failed. The rules only apply to coalition members; industry opt-outs are fragile and easily overridden; industry opt-outs only address usage and do not impose meaningful collection or retention limitations; and notice and privacy interfaces were seriously flawed.[22]

Companies have also pushed back against the CCPA. Last year, the tech industry worked to remove CCPA controls over third-party targeted advertising by supporting SB 753, which would have completely exempted cross-context targeted advertising from the opt-out.[23] More recently, advertising groups have asked the AG to delay enforcement of the law—even though they've had over a year to get into compliance.[24] Other states, under pressure from the tech industry, have pursued opt-out bills with a much more limited definition of sale.[25] The AG should not let companies continue to try to evade meaningful regulation.

Impact on consumers

Over time, behavioral advertising has become increasingly invasive. Sites are able to track every move a consumer makes online, including search history and search terms.[26] Apps, too, track and sell consumers' most sensitive data. Recent research from Consumer Reports revealed that so-called health apps such as period trackers collect information not only about how often you menstruate, but whether you're trying to have a baby, and even how often you have sex. Unless Californians opt out of the sale of their information—and the companies involved honor the opt-out—that information could find its way to third parties, and could be further sold or otherwise disseminated in ways that could mean getting charged more for insurance, or even facing job discrimination.[27] This information is often widely traded as a matter of course. Another recent study found that 10 apps together sent personal information on consumers to at least 135 companies involved in advertising and behavioral profiling.[28]

---

[22] *Statement of Justin Brookman Before the U.S. Senate Comm. On Commerce, Sci., and Transp.*, CTR. FOR DEMOCRACY & TECH. (Apr. 24, 2013), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.
[23] *California Consumer Privacy Act Update: Assembly Approves 12 Amendments - Changes Would Exclude Employees and Vehicle Information, Protect Loyalty Programs*, JD SUPRA (Jun. 7, 2019), https://www.jdsupra.com/legalnews/california-consumer-privacy-act-update-48943/.
[24] Andrew Blustein, Ad Industry Calls for Delayed Enforcement of CCPA, THE DRUM (Jan. 29, 2020), https://www.thedrum.com/news/2020/01/29/ad-industry-calls-delayed-enforcement-ccpa.
[25] See, e.g., Nevada SB 220 (2019), https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Text; Arizona HB 2729 (2020), https://apps.azleg.gov/BillStatus/BillOverview/73672.
[26] Glenn Fleischman, *How The Tragic Death of Do Not Track Ruined the Web for Everyone*, FAST COMPANY (Mar. 19, 2019), https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone [hereinafter *The Tragic Death of Do Not Track*].
[27] Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPORTS (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.
[28] OUT OF CONTROL, *supra* note 4, at 5.

Consumers are actively engaged online, spending around six hours per a day using digital media, mostly on mobile devices.[29] While some consumers may well appreciate receiving targeted offers, in study after study, the majority of people do not wish to be tracked in order to be served with more relevant advertising.[30] In a recent Pew Research study, 86% of users reported taking some action to mask their digital footprints, but most wish they had the ability to do more.[31] Older, less tech-savvy users especially feel powerless to take responsibility for protecting their privacy.[32] Most people just don't want their personal information sold to countless strangers without their knowledge,[33] and at the very least companies should be required to honor affirmative efforts to opt out of the ad tech ecosystem.

The AG should remove the limits on the definition of personal information, which would create a significant loophole for targeted advertising.

The AG should delete the provision in § 999.302, which exempts IP addresses from the definition of personal information. While information that can't be tied to a single, identifiable person should not necessarily be subject to access or deletion requests, particularly without controls to ensure that one's search terms are being shared with another person, if companies are using that data to target ads, it's identifiable and eliminating it from the definition of personal information is contrary to the clear language of the statute.[34] Consumers should retain opt-out rights in this case. This new provision significantly weakens the privacy protections of the CCPA and is essentially a loophole for targeted advertising.

IP addresses, even though they appear to be "anonymous," allow companies to access a significant amount of data about consumers and their families. While IP addresses assigned to consumers are often *dynamic* (in that they are periodically rotated), these numbers may in

[29] Ginny Marvin, *Digital Advertising's Opportunities & Threats from Mary Meeker's Internet Trends Report*, MARKETING LAND (June 1, 2018), https://marketingland.com/digital-advertisings-opportunities-threats-from-mary-meekers-internet-trends-report-241264.
[30] Chris Jay Hoofnagle et al., *Privacy And Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection Of Data About Their Online Activities*, AMSTERDAM PRIVACY CONFERENCE (Oct. 8, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135; Kristin Purcell et al., *Search Engine Use Over Time*, PEW RESEARCH CTR. (Mar. 9, 2012), http://www.pewinternet.org/2012/03/09/main-findings-11/; J. Turow et al., *Americans Reject Tailored Advertising And Three Activities That Enable It*, SSRN (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
[31] Lee Raine, *The State of Privacy In Post-Snowden America*, PEW RESEARCH CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.
[32] Fatemeh Khatibloo, *Marketers, Here's How Your Customers Feel About Privacy*, FORBES (Dec. 16, 2016), https://www.forbes.com/sites/forrester/2016/12/16/marketers-heres-how-your-customers-feel-about-privacy/#52356c0f18e4.
[33] Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; Joseph Turow et al., The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation, Annenberg School for Communication, University of Pennsylvania (Jun. 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.
[34] Cal. Civ. Code §1798.140(o)(1)(A).

practice not be changed for months at a time; and as companies migrate to IPv6 addresses, there may be no need to rotate IP addresses at all as IPv6 effectively eliminates the problem of address scarcity. It can easily be used to track user behavior over time, even without access to cookies or other identifiers.[35] Moreover, correlation of IP addresses allows companies to engage in cross-device tracking, as devices that share local networks are considerably more likely to be operated by the same persons—meaning that they're used to develop detailed profiles about consumers, across devices, and about those with whom they live and spend time, for ad targeting purposes.[36] 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.

This new provision goes far beyond the Attorney General's rulemaking authority. Section 1798.185 gives the AG the authority to issue rules to further the purposes of the title, which are, in turn, to further Californians' constitutional right to privacy.[37] Significantly weakening the definition of personal information would go against the AG's remit under the CCPA. IP addresses are explicitly included in the CCPA's definition of personal information,[38] and to remove them clearly subverts legislative intent. Finally, a bill to accomplish the same goals as provision § 999.302—to exempt IP addresses from the protections of the CCPA—was properly defeated in the California legislature in July.[39] It would be inappropriate for the AG to overrule the legislature by inserting this provision now.

The AG should make global opt-outs more user-friendly.

We appreciate that the AG has kept the requirement that companies must honor browser privacy signals as an opt-out of sale.[40] Forcing consumers to opt out of every company, one by one—including from data brokers, whom consumers may not even know are collecting their data—is simply not workable. However, the current draft should be adjusted to ensure that it is consumer-friendly. The AG should state that platform-level controls to limit data sharing should be interpreted as CCPA opt-outs, including Do Not Track and Limit Ad Tracking. Or at the very least, the AG should clarify how platforms can certify that new or existing privacy settings should be construed as CCPA opt-outs.

First, the AG should make it explicit in the rules that enabling Do Not Track opts the consumer out of the sale of their information. Instead, the updated draft regulations require browser signals

[35] 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.
[36] *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.
[37] Cal. Civ. Code §1798.175.
[38] Cal. Civ. Code §1798.140(o)(1)(A).
[39] AB 873 (2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB873.
[40] § 999.315(d).

to clearly convey that it constitutes an opt-out of sale, and require consumers to actively indicate their choice to opt-out.[41] This language unduly restricts consumer agency, particularly because it would mean that signing up for Do Not Track—likely the most well-known privacy setting, at one time adopted by Safari, Internet Explorer, Chrome, and Firefox—would not opt consumers out of sale.[42] While we do not object to the requirement in the draft regulations that opt-out settings should be off by default, consumers would reasonably expect that enabling Do Not Track would opt them out of sale to third parties. Consumers shouldn't have to take an additional step to opt out of sale after they enable DNT or a similar setting. This would mean that consumers already using DNT—by one estimate, nearly a quarter of American adults—would be much less likely to benefit from the AG rule, since they would likely assume that they had already opted out of sale.[43]

But DNT isn't the only platform-level privacy setting governing third-party sharing. To encourage the development and awareness of, and compliance with, privacy settings for other platforms, we urge the AG to issue rules governing: 1) how the developer of a platform may designate a particular privacy control to be deemed a valid request; 2) how the attorney general shall maintain and publish a comprehensive list of privacy controls to be deemed valid requests; and 3) the conditions under which business may request an exception to sell data notwithstanding a consumer's valid request.

Millions of consumers have signed up for Do Not Track, but there are other settings that are far less well known, in part because they're not associated with online use. For example, Apple, in 2013 introduced a mandatory "Limit Ad Tracking" setting for iPhone applications, and even improved that tool to further limit the information advertisers can receive when the setting is activated.[44] Consumers also need global opt-outs from sale when using their smart televisions and voice assistants. In order to better raise awareness of the different options on the market, to encourage the development of new tools, and to address the lack of clarity around which browser settings must be honored as opt-outs, the AG should set up a system in order to make this clear for consumers and businesses.

[41] § 999.315(d)(1).
[42] *See, The Tragic Death of Do Not Track*, *supra* note 26. While it is true that in 2012, Microsoft enabled DNT in its Internet Explorer browser by default that was discontinued in 2015 following sustained criticism.
[43] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, GIZMODO (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.
[44] Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You*, BUS. INSIDER (Sept. 10, 2016), http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9.

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

Consumers shouldn't be forced to choose between affordable necessities and exercising their right to privacy. Unfortunately, the CCPA suggests 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.[45] This language was added to the CCPA over objections from advocates, who argued that consumers should not be penalized for exercising their privacy rights.[46] While consumers may expect to have their purchases tracked by a company to be rewarded for repeated patronage, selling that consumer data to third parties runs counter to what participating consumers would reasonably expect.

To prevent some of the worst abuses associated with financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The CCPA prohibits financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.[47] And, the AG currently has the authority under the CCPA to issue rules with respect to financial incentives.[48] Thus, we urge the AG to exercise its authority to prohibit the use of financial incentives in market sectors that lack competition. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates—about $30 per month—for not leveraging U-Verse data for ad targeting.[49] 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,[50] further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.[51] The AG should exercise its authority to put reasonable limits on these programs in consolidated markets.

[45] Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).
[46] 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.
[47] Cal. Civ. Code § 1798.125(b)(4).
[48] Cal. Civ. Code § 1798.185(a)(6).
[49] 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/.
[50] *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.
[51] *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets*, FED. TRADE COMM'N (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

The AG should require companies to forward opt-out requests to third parties to whom it has sold data, if they have the information to do so.

To make the CCPA workable for consumers, there must be some obligation on companies to facilitate opt-out requests within the data-sharing ecosystem. In the previous draft of the proposed rules, companies were required to notify all third parties to whom it had sold data, when it received an opt-out request from a consumer. Under the updated rules, companies only need notify those with whom the information was sold after opt-out request was received.[52] The new rule is too limited. Where possible, companies should be required to forward opt-out requests.

Since companies may have sold data to any number of companies without a consumer's knowledge—including data brokers, with which consumers have no direct relationship—the updated rule significantly undermines consumers' ability to protect their privacy. Further, the CCPA doesn't require transparency about the precise third parties to which data is sold.[53] While companies may not always maintain detailed records on all of the companies with whom they have sold data, especially in adtech transactions in which data is potentially transferred with hundreds of companies in a fraction of a second, if the company knows who it has sold the data to, they should be required to forward the opt-out request.

The AG should consider placing a retention limit on records of deletion.

The draft rules have been amended to allow companies to hold onto a deletion request, to help ensure that the personal information remains deleted.[54] We suggest that the AG consider placing a retention limit on these records, since the very fact of having an account with a company—for example, Ashley Madison, Tinder, and Grindr—can reveal more about a person than they might like others to know.[55]

Given the plethora of data breaches—Privacy Rights Clearinghouse has tracked nearly 10,000 since 2006[56]—and the fact that it's not clearly stated in the CCPA that a company can't sell the information retained about a consumer following a deletion request, companies shouldn't be able to hold onto that information indefinitely. Further, the rationale that the record of deletion needs to be retained to ensure that information stays deleted is not entirely convincing, as a deletion request is not the same as a prohibition on collection—a company could conceivably collect information about a consumer again.

---

[52] § 999.315(f).
[53] Cal. Civ. Code §1798.110(4).
[54] § 999.313(d)(5).
[55] Thomas Germain, *How Private Is Your Online Dating Data?* CONSUMER REPORTS (Sept. 21, 2019), https://www.consumerreports.org/privacy/how-private-is-your-online-dating-data/.
[56] Privacy Rights Clearinghouse, Data Breaches (last visited Feb. 23, 2020), https://privacyrights.org/data-breaches.

The AG draft rules appropriately address household-level access and deletion requests.

The updated rules allow companies to honor access and deletion requests of unauthenticated or household-level data, when all the members of the household have placed a request jointly, and have verification their identities.[57] While this is a high bar to meet, avoiding risk of unwanted disclosure of information is important. Transparency, data portability, and access rights are key protections, but without a high bar to verify that all members of the household are comfortable with the request, 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,[58] 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. 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. Not only could this be harmful to a consumer's privacy, but also it could facilitate identity theft. Identity theft by family members is a serious problem, by one estimate totaling approximately one-third of instances of identity theft overall.[59]

Thank you for the opportunity to submit comments on the updated draft rules. We would be happy to address any questions you have.

Respectfully submitted,

Maureen Mahoney
Policy Analyst
San Francisco, CA

Justin Brookman
Director, Privacy and Technology Policy
Washington, DC

[57] § 999.318
[58] Cal. Civ. Code § 1798.110(d)(2).
[59] Bruce Kennedy, *When Identity Theft is a Family Affair,* CBS NEWS (Apr. 14, 2014), https://www.cbsnews.com/news/when-identity-theft-is-a-family-affair/.