epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CALIFORNIA OFFICE OF THE ATTORNEY GENERAL

NOTICE OF PROPOSED RULEMAKING

THE CALIFORNIA CONSUMER PRIVACY ACT

December 6, 2019

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Notice of Proposed Rulemaking Action on the California Consumer Privacy Act ("CCPA").[1] EPIC thanks the Office of the Attorney General for its work on the proposed regulations and leadership on privacy issues.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has long supported the establishment of comprehensive federal privacy law and also argued that federal law should not preempt stronger state laws.[3] EPIC recently released *Grading on a Curve: Privacy Legislation in the 116th*

[1] California Department of Justice, Notice of Proposed Rulemaking Action, Title 11 (Oct. 11, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf.
[2] *About EPIC*, EPIC (2019), https://www.epic.org/epic/about.html.
[3] *See* Privacy in the Commercial World, H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection (testimony of Marc Rotenberg, Exec. Dir., EPIC) (March 1, 2001), https://epic.org/privacy/testimony_0301.html; *Hearing on the Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach*, H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade (testimony of Marc Rotenberg, Exec. Dir., EPIC) (June 15, 2011), https://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf; *Reauthorizing Brand USA and the U.S. SAFE WEB Act*, H. Comm. on Energy & Commerce, Subcomm. on Consumer Protection & Commerce (statement of EPIC) (Oct. 29, 2019), https://epic.org/testimony/congress/EPIC-HEC-SafeWebAct-Oct2019.pdf. *See, e.g.,* Video Privacy Protection Act of 1988, 18 U.S.C. 2710(f) ("The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.")

Congress.[4] EPIC's report sets out the key elements of a comprehensive federal privacy law: (1) strong definition of personal information; (2) establishment of an independent data protection agency; (3) individual rights; (4) strong data controller obligations; (5) algorithmic transparency; (6) data minimization and privacy innovation; (7) prohibits take-it-or-leave it and pay-for-privacy terms; (8) private right of action; (9) limits government access to personal data; and (10) does not preempt stronger state laws.

As the Attorney General considers ways to improve the text of the proposed California state regulations, EPIC submits these comments to evaluate how the proposal meets the framework criteria EPIC has proposed to the Congress.

Strong definition of personal information

EPIC commends the Attorney General's defense of a robust definition of personal information. The CCPA is the culmination of state-wide support from voters "to empower consumers to find out what information businesses were collecting on them and give them the choice to tell businesses to stop selling their personal information."[5] The California Legislature has "explained that an individual's ability to control the use and sale of their personal information was fundamental to the 'inalienable' right of privacy set forth in the California Constitution."[6] With these objectives in mind, the California Legislature has incorporated a strong definition of "personal information" into the Act.[7]

[4] *See* https://epic.org/GradingOnACurve/.

[5] CALIFORNIA SENATE JUDICIARY COMMITTEE, CALIFORNIA BILL ANALYSIS, S.B. 1121 Sen. (2018); *cf.* EPIC, *Public Opinion on Privacy*, https://epic.org/privacy/survey/.

[6] *California Department of Justice, Notice of Proposed Rulemaking Action*, at 9 (Oct. 11, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf.

[7] *See* Cal. Civ. Code §999.301; *reprinted in* Marc Rotenberg, THE PRIVACY LAW SOURCEBOOK 2020 (EPIC 2020).

The scope of a privacy bill is largely determined by the definition of "personal information." A good definition includes both data that is explicitly associated with a particular individual and also data from which it is possible to infer the identity of a particular individual. Personal information also includes all data about an individual, including information that may be publicly available, such as zip code, age, gender, and race.[8] All of these data elements are part of the consumer profiles companies create and provide the basis for decision-making about the individual. EPIC supports the California Legislature's broad definition of "personal information."

The AG should not modify the Act's strong definition of "personal information." The Act's definition of "personal information" is comprehensive and should not be modified. Furthermore, the AG should not endorse any proposed changes to the Act currently under consideration by the California Legislature, such as Assembly Bill 873 (AB-873).[9] Proposed changes to the Act in AB-873 add qualifying "reasonably" language to various definitions, including the definition of "personal information," which undermine the current definition in the Act and weakens data privacy protections for Californians.

Establishment of an Independent Data Protection Agency

Almost every democratic country in the world has an independent national data protection agency, with the competence, authority, and resources to help ensure the protection of personal data. These agencies act as an ombudsman for the public. Many now believe that the failure to establish a data protection agency in the U.S. has contributed to the growing incidents

[8] EPIC Comments to FCC, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 18-19 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002079241.pdf.
[9] *See* AB-873, Cal. Leg., 2019–20 Regular Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB873.

of data breach and identity theft.[10] EPIC has long supported the establishment of a federal data protection agency.[11]

A strong state privacy law would establish an independent state-level Data Protection Agency with resources, technical expertise, rulemaking authority and effective enforcement powers. EPIC commends the Attorney General's work on privacy issues, but recognizes that resource limitations and competing priorities of the office will make effective enforcement of California privacy rights difficult to do alone. An expert agency would be able to assist the AG with this critical responsibility. The California Privacy Rights and Enforcement Act of 2020 would establish a California Privacy Protection Agency that would assume rulemaking responsibilities, promote public awareness, provide guidance to consumers and businesses, provide technical assistance to the legislature, and cooperate with other agencies on consistent application of privacy protections.[12] EPIC recommends that the Attorney's General's office work in support of a California privacy agency.

Individual rights (right to access, control, delete)

Californians have strong individual rights under the Act, which EPIC supports.[13] Privacy legislation must give individuals meaningful control over their personal information held by others. This is accomplished by the creation of legal rights that individuals exercise against

[10] *Examining Legislative Proposals to Protect Consumer Data Privacy*, S. Comm. on Commerce, Sci., and Trans. (statement of EPIC) (Dec. 4, 2019); https://epic.org/testimony/congress/EPIC-SCOM-LegislativePrivacyProposals-Dec2019.pdf; *see also* EPIC, The U.S. Urgently Needs a Data Protection Agency, https://epic.org/dpa/.

[11] Marc Rotenberg, *In Support of a Data Protection Agency in the United States,* 8 Government Information Quarterly 79-93 (1991)

[12] Alastair Mactaggart, letter to Office of the Attorney General Initiative Coordinator re Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment) Nov. 13, 2019, https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

[13] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev.

companies that choose to collect and use their personal data. These rights typically include the right to access and correct data, to limit its use, to ensure it is security protected, and also that it is deleted when no longer needed. These rights are present in the CCPA. “Notice and consent” has little to do with privacy protection. This mechanism allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual. The proposed regulations maintain the individual rights granted to consumers in the Act, and EPIC supports the AG’s decision to uphold them. Section 1798.100 of the Act grants the individual “right to know,” Section 1798.130 grants the individual “right to access” and Section 1798.105 grants the individual “right to delete.”[14]

Strong data controller obligations

Organizations that choose to collect and use personal data necessarily take on obligations for the collection and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Together with the rights of individuals describes above, they are often described as “Fair Information Practices.” Many of these obligations are found today in U.S. sectoral laws, national laws, and international conventions. These obligations include:

- Transparency about business practices
- Data collection limitations
- Use/disclosure limitations
- Data minimization and deletion
- Purpose specification
- Accountability
- Data accuracy
- Confidentiality/security

[14] Cal. Civ. Code §§ 1798.100, 105, 130.

The CCPA lacks several of these key provisions. For example, it lacks a presumption against disclosure, data security standards, and accountability mechanisms. The Legislature must update the CCPA to place responsibilities on companies.

Require Algorithmic Transparency

The California AG should require data brokers to identify the factors used in algorithmic decision-making practices. As automated decision-making has become more widespread, there is growing concern about the fairness, accountability, and transparency of algorithms.[15] All individuals should have the right to know the basis of an automated decision that concerns them. Modern day privacy legislation typically includes provisions for the transparency of algorithms to help promote auditing and accountability.[16]

Data broker registry requirements were incorporated into the Act in October 2019 in AB-1202. Under Cal. Civ. Code § 1798.99.82(b)(2)(B), data brokers are requires to provide "any additional information or explanation the data broker chooses to provide concerning its data collection practices."[17] EPIC supports this provision of the Act, but it is only the first step to transparency because it neither requires data brokers to provide information about the algorithms they use, nor the factors they incorporate into their data collection, management, and decision-making practices.[18] The AG should require data brokers to provide this information in order to

[15] *The Fair Housing Act: Reviewing Efforts to Eliminate Discrimination and Promote Opportunity in Housing*, H. Comm. on Financial Services (statement of EPIC) (Apr. 2, 2019), https://epic.org/testimony/congress/EPIC-HFS-FairHousingAct-Apr2019.pdf.

[16] EPIC, Algorithmic Transparency: End Secret Profiling, https://epic.org/algorithmic-transparency/; The Public Voice, *Universal Guidelines for Artificial Intelligence*, https://thepublicvoice.org/AI-universal-guidelines.

[17] Cal. Civ. Code § 1798.99.82(b)(2)(B).

[18] *See Universal Guidelines for Artificial Intelligence*, PUB. VOICE (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/; EPIC, *The Code of Fair Information Practices*, https://epic.org/privacy/consumer/code_fair_info.html.

raise consumer awareness of how their personal data is being used and collected, as well as bring to light secret profiling systems which should be prohibited.

Data brokers that generate consumer scores must be required to reveal the factors that used to generate scores. There are many data brokers that generate "secret scores" about consumers which they track and sell to other companies.[19] These data brokers are "largely invisible to the public" and "most people have no inkling they even exist."[20] These companies make decisions that impact the ability of people to obtain jobs, credits, housing, and healthcare. Fortunately, these companies are covered by the Act and do not fall within the consumer reporting and financial institution exceptions.[21] Coverage must be preserved by the AG rulemaking.

Require Data Minimization and Privacy Innovation

Many U.S. privacy laws have provisions intended to minimize or eliminate the collection of personal data. Data minimization requirements reduce the risks to both consumers and businesses that could result from a data breach or cyber-attack.[22] Good privacy legislation should also promote privacy innovation, encouraging companies to adopt practices that provide useful services and minimize privacy risk. Privacy Enhancing Techniques ("PETs") seek to minimize the collection and use of personal data. The Legislature should consider adding data minimization requirements in a future update of the Act.[23]

[19] Kashmir Hill, *I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too* N.Y. Times (Nov. 5, 2019), https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html.
[20] *Id.*
[21] *See e.g., Can I use Sift for credit risk reporting?* SIFT, https://support.sift.com/hc/en-us/articles/202713053-Can-I-use-Sift-for-credit-risk-prediction- (last visited Dec. 5, 2019).
[22] EPIC Comments to Gov't of India, *White Paper of the Committee of Experts on a Data Protection Framework for India* 3 (Jan. 2018), https://epic.org/EPIC-IndiaDataProtection-Jan2018.pdf.
[23] *See* S. 1214, 116th Cong. § 12 (2019).

Prohibit take-it-or-leave-it or pay-for-privacy terms

Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.[24] Generally, the CCPA does not allow businesses to "discriminate against a consumer because the consumer exercised any of their . . . rights under [the Act]."[25] However, the Act allows businesses to offer pay-for-privacy "financial incentives" to consumers, so long as they are "reasonably related to the value provided to the consumer by the consumer's data."[26] EPIC opposes this pay-for-privacy exception in the Act, which is in violation of California's inalienable right to privacy, encourages consumer discrimination, and should be mitigated to the maximum extent available by the AG's rulemaking authority.[27]

The AG's proposed regulations require businesses to notify consumers of financial incentives in language "that is easy to read and understandable to an average customer."[28] Businesses that use financial incentives are also required to explain price or service differences to consumers.[29] Specifically they must provide "[a] good-faith estimate of the value of the consumer's data that forms the basis for" the financial incentive, and they must describe the method the business used to calculate the value of the consumer's data."[30] Short of an outright ban on pay-for-privacy, EPIC encourages the AG to consider additional language to strengthen

[24] *See* Marc Rotenberg, *Privacy Guidelines for the National Research and Education Network*, NCLIS (1992) ("Users should not be required to pay for routine privacy protection. Additional costs for privacy should only be imposed for extraordinary protection.") *reprinted in* Anita L. Allen & Marc Rotenberg, PRIVACY LAW AND SOCIETY 762 (2016); *see also* Marc Rotenberg, *Communications Privacy: Implications for Network Design,* 36 Communications of the ACM 61-68 (Aug. 1993).
[25] Cal. Civ. Code § 1798.125(a)(1).
[26] Cal. Civ. Code §§ 1798.125(a)(2), (b)(1).
[27] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy.").
[28] Proposed Regs. § 999.307(a)(2).
[29] Proposed Regs. § 999.307(b)(5).
[30] Proposed Regs. § 999.307(b)(5).

the notice requirement in order to further deter businesses from harming consumers through excessive financial incentives.

Financial incentive calculation of the value of consumer data should be equal among all consumers. Most concerning in the proposed regulations are businesses ability to charge different prices based on consumer data.[31] The proposed regulations permit businesses to calculate the value of consumer data based on "separate tiers, categories or classes of consumers."[32] This is highly discriminatory and should be struck from the regulations. A recent report from the Australian Competition and Consumer Commission (ACCC) found that "[a] consequence of increasingly sophisticated data analytics and personalisation is that it may enable and encourage highly targeted price discrimination."[33] Specifically, businesses create highly detailed profiles on consumer "behaviours and attributes to offer each a different price for a product or service."[34] Allowing such categorization of consumers under the regulations have discriminatory effects against protected classes of Californians. For example, a recent University of California Berkeley study found that mortgage lenders profit 11.5% more on average from Latinx and African-American borrowers than other borrowers.[35]

Under the current proposed regulation, these businesses would be permitted to value Latinx and African-American consumer data higher than that other consumer classes, resulting in price discrimination. For households with limited financial resources, they may be left with no

[31] *See* Cal. Civ. Code § 1798.125.

[32] Proposed Regs. § 999.337(b)(3).

[33] Customer Loyalty Schemes, ACCC (Dec. 2019), https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF.

[34] Customer Loyalty Schemes, ACCC (Dec. 2019), https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF.

[35] https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf

alternative but to surrender to allowing businesses to use, share, and sell their personal data. To mitigate against these potential discriminatory practices, the AG should remove Section 999.337(b)(3) from the regulations and require businesses to calculate and apply data privacy financial incentives for all of its customers equally.

Private Right of Action

Privacy laws in the U.S. typically make clear the consequences of violating a privacy law. Statutory damages, sometimes called “liquidated” or “stipulated” damages are a key element of a privacy law and should provide a direct benefit to those whose privacy rights are violated.[36] The Legislature should consider expanding the Act’s limited private right of action to include all violations of the Act. The Attorney General alone cannot meaningfully enforce the privacy rights of all Californians.

Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government would be able to collect personal data in bulk from companies, a form of mass surveillance enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[37] California has the strongest law about warrantless

[36] *See* Hearing on “Cybersecurity and Data Protection in the Financial Sector,” H. Comm. on Financial Services 7-8 (testimony of Marc Rotenberg, Exec. Dir., EPIC) (Sept. 2011), https://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.
[37] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

surveillance in the nation: the California Electronic Communications Privacy Act. The AG should continue to use its authority enforce CalECPA.[38]

The proposed regulations signal that the AG intends to maintain strong data privacy protections in the CCPA for Californians. EPIC supports the AG's leadership on privacy issues and work on the proposed regulations.

Sincerely,

/s/ *Marc Rotenberg* Marc Rotenberg EPIC President	/s/ *Christine Bannan* Christine Bannan EPIC Consumer Protection Counsel
/s/ *W. Hunter Daley* W. Hunter Daley EPIC Law Clerk	

[38] Electronic Communications Privacy Act, CAL. PENAL CODE § 1546.4(b) (2016).