epic.org

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

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

California Privacy Protection Agency

on

Invitation for Preliminary Comments

Notices & Disclosures and Employee Data

May 20, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the invitation of the California Privacy Protection Agency ("Agency" or "CalPrivacy") for preliminary comment on notices, disclosures, and employee data, published on April 20, 2026.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has previously provided comments on the California Consumer Privacy Act (CCPA),[3] published a detailed analysis of the California Privacy Rights Act before its approval by

---

[1] Invitation for Preliminary Comments: Notices & Disclosures and Employee Data, Cal. Privacy Protection Agency (Apr. 20, 2026), https://cppa.ca.gov/regulations/pdf/notices_disclosures_employee_data.pdf.
[2] *About Us*, EPIC, https://epic.org/about/ (2025).
[3] Comments of the Electronic Privacy Information Center (EPIC) and the Consumer Federation of America (CFA) in Response to the California Privacy Protection Agency's Proposed Rulemaking Regarding Cybersecurity, Risk Assessments, and Automated Decisionmaking Technology (Feb. 19, 2025), https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/; Comments of Consumer Reports, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) and Privacy Rights Clearinghouse (PRC) In Response to the California Privacy Protection Agency's Invitation for Preliminary Comments On Proposed Rulemaking Under Senate Bill 362 (June 25, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/06/Comments-of-Consumer-Reports-In-Response-to-the-California-Privacy-Protection-Agencys-Invitation-for-Preliminary-Comments-On-Proposed-Rulemaking-Under-Senate-Bill-362.pdf; Comments Of The Electronic Privacy Information Center, Center For Digital Democracy, and Consumer Federation Of America, to the California Privacy Protection Agency (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/; Comments of EPIC to Cal. Privacy Prot. Agency (Nov. 20, 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-CPPA-Comments-Nov-20.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Aug. 23, 2022), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Nov. 8, 2021), https://epic.org/wp-content/uploads/2021/11/PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf; Comments of

California voters,[4] and presented oral testimony to the Agency to encourage the strongest protections for Californians.[5]

The CCPA established important rights for Californians to know, correct, delete, and opt out of sale of information, and includes strong data minimization requirements to protect Californians from harmful overcollection of personal information, out-of-context impermissible secondary data uses, and excessive data retention.[6] Because privacy policies and disclosures are the primary means for data subjects and the public to understand the practices of the covered entities, they should be as clear as possible and directly tied to actionable steps for Californians to exercise their rights under the CCPA. EPIC asks the Agency to consider the following suggestions to that end:

- Privacy policies should be easily accessible and consolidated in one easy-to-find link rather than spread out across many documents through multiple links;
- Covered entities should provide all published versions of privacy policies, with their effective dates, in an easily accessible manner; and
- Policies and disclosures should directly link to where individuals can exercise their rights under the CCPA, and these regulations should prohibit dark patterns.

These recommendations should apply to privacy policies and disclosures for consumers and workers alike, and EPIC also echoes the comments submitted by the Berkeley Labor Center on worker privacy.

Privacy policies should be accessible and should not span a web of documents. As a recent Stanford study on the privacy policies of six frontier AI model developers has found, all of the developers rely upon a web of documents in addition to their primary privacy policies to govern their

---

EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf.

[4] EPIC, California's Proposition 24 (2020), https://epic.org/californias-proposition-24/.

[5] EPIC Calls Out CPPA as Board Votes to Adopt Weak Risk Assessment, ADMT, and Cybersecurity Regulations, EPIC (July 24, 2025), https://epic.org/cppa-votes-to-adopt-weak-cybersecurity-risk-assessments-and-admt-regulations/.

[6] EPIC, *Data Minimization*, https://epic.org/issues/consumer-privacy/data-minimization/; EPIC, *California Consumer Privacy Act (CCPA)*, https://epic.org/california-consumer-privacy-act-ccpa/.

use of users' chat data, with OpenAI relying on at least six different policies.[7] Finding, reading, and synthesizing six different privacy policies is untenable for an ordinary person and undermines Californians' ability to effectively exercise their rights under the CCPA. Some of these policies also have ambiguous language that states that the entity "may" use data collected across other products owned by the umbrella company to train AI models,[8] which clouds transparency around which data categories from which products are used this way. These sorts of sprawling webs of difficult-to-parse privacy policies and disclosures are common across many companies, and CalPrivacy should consider adopting regulations that would prohibit these practices.

Multiple privacy policies and disclosures can also lead to overlapping and conflicting messages about the company's policies and the data subject's rights. For example, in *Calhoun v. Google*, Google argued that an individual's "agreement" to their Privacy Policy and Google Account Holder agreements meant that they had consented to all potential data collection described not only in the policies and agreements, but also in any other linked disclosures, FAQs, and other documents.[9] Google contended that even when it has explicitly promised its users that it will protect their data, it didn't have to abide by that promise so long as it points to contrary terms in its general user agreement and statements posted in a sprawling web of disclosure pages.[10] Google's arguments did not succeed in the Ninth Circuit because when the disclosures are read together, "a reasonable user would not necessarily understand that they were consenting to the data collection at issue."[11] Overlapping and conflicting policies thus increase the burden on individuals attempting to understand the data practices of the entity and undermine their privacy rights by potentially misleading them. The Agency should develop regulations that place the burden on the covered entity to ensure its policies and disclosures are internally coherent and kept to a minimum number of

---

[7] Jennifer King, Kevin Klyman, Emily Capstick, Tiffany Saade and Victoria Hsieh, *User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies*, arXiv (Sept. 5, 2025), https://arxiv.org/abs/2509.05382.
[8] *Id*.
[9] Brief for the Elec. Priv. Information Ctr. as Amicus Curiae in Support of Plaintiffs-Appellants and Reversal, Calhoun v. Google, _ F.4th _, 2024 WL 3869446 (9th Cir. 2024) (No. 22-16993).
[10] *Id.*
[11] *Id*.

documents and that there is accountability if covered entities publish conflicting or deceptive policies.

Another aspect of privacy policies and disclosures that make them untenable for data subjects and the public to understand is their ever-changing nature. As a recent whitepaper by EPIC Counsel Caroline Kraczon and EPIC Scholar in Residence Justin Sherman on manipulative design elements in consumer opt-out processes points out, researching privacy policies is difficult in part because privacy policies are difficult to archive, and are often replaced by new versions.[12] There is often no clear way to compare prior versions of privacy policies and disclosures. The Agency should consider rules that require covered entities to post accessible links to previous versions of privacy policies and other disclosures with dates when the policies were in effect and changes noted so that consumers can easily decipher the new terms.[13]

Lastly, privacy policies and disclosures should provide actionable steps to Californians. Regulations on privacy policies and disclosures should require direct links to where individuals can exercise their rights under the CCPA, and they should prohibit manipulative design practices. As EPIC's whitepaper points out, some websites also offered no clear way to exercise opt-out rights.[14] Further, many of the companies surveyed exhibited some evidence of manipulative design in the opt-out process, including confusing or contradictory language.[15] Regulations should address confusing or misleading language in policies and disclosures, such as those that suggest key functionalities will not be available or that exercising their rights would be futile.[16] Requiring direct

[12] Caroline Kraczon & Justin Sherman, EPIC, *Good Luck Opting Out: Manipulative Design Patterns in Opt-Out Processes* 26–27 (May 2026), https://epic.org/wp-content/uploads/2026/05/Good-Luck-Opting-Out-Manipulative-Design-Patterns-in-Opt-Out-Processes.pdf.
[13] For example, see EPIC's privacy policy for its own website. *Updates to EPIC's privacy policy posted on July 26*, 2024, EPIC (July 26, 2024), https://epic.org/wp-content/uploads/2024/07/EPIC-changes-to-privacy-policy.pdf.
[14] Kraczon & Sherman, *supra* note 12, at 27–28, 35-36.
[15] *Id*. at 30–33. *See also* EPIC, Comments to the Colo. Dept. of Law on Proposed Rulemaking Under the Colorado Privacy Act of 2021 (Aug. 5, 2022), https://epic.org/documents/epic-comments-on-colorado-privacy-act-rulemaking/.
[16] Kraczon & Sherman, *supra* note 12, at 30–33.

links in privacy policies and disclosures would be a straightforward way to lessen the burden on Californians who are trying to exercise their CCPA rights.

When Californians encounter hard-to-understand privacy policies and friction while trying to exercise their privacy rights, the important work that California has done to enshrine privacy rights into law is undermined. We hope that EPIC's whitepaper aids CalPrivacy in its efforts to ensure that Californians can exercise their privacy rights. We thank CalPrivacy for the opportunity to provide preliminary comment on this topic, and we look forward to working with the Agency in the future to continue protecting the privacy of all Californians.

Respectfully Submitted,

/s/ Mayu Tobin-Miyaji
Mayu Tobin-Miyaji
EPIC Law Fellow
tobin-miyaji@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)