
CALIFORNIA PRIVACY PROTECTION AGENCY

400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov



STATE OF CALIFORNIA

California Privacy Protection Agency Board**Informational Session****Notices, Disclosures, and Privacy Rights: A Review of Challenges and Opportunities Within California's Consumer Privacy Framework**

November 5, 2026

Background Information

The California Consumer Privacy Act (CCPA) and the California Privacy Protection Agency's (Agency) implementing regulations require businesses to provide consumers with clear and accessible notices describing their privacy practices. In addition, the CCPA and the regulations require businesses to provide consumers with specific rights with respect to the personal information businesses collect about them. Although consumers must take action to exercise their CCPA rights, the CCPA directs the Agency to establish rules to help minimize burdens on consumers as they do so.

Even with these rights and protections, the Agency continues to receive feedback that consumers are frustrated. Specifically, consumers struggle to navigate and understand privacy policies and other disclosures, and they experience friction when exercising their privacy rights. Accordingly, in November 2025 the Agency's Board directed the Legal Division to conduct preliminary rulemaking to assess whether regulatory changes are necessary to address these issues. In March and April 2026, the Agency invited preliminary public comments on two topics: (1) Notices and Disclosures, and (2) Reducing Friction in the Exercise of Privacy Rights.

As background for the informational session on November 5, 2026, this document outlines the legal requirements under the CCPA and existing regulations related to notices and disclosures, as well as friction in exercising privacy rights. It also provides a summary of the topics that will be covered by the four speakers invited to present at this informational session.

Notices and Disclosures

The CCPA grants consumers enumerated privacy rights, including the rights to know, delete, correct, limit the use and disclosure of sensitive personal information, opt-out of sale or sharing, and be free from discrimination for exercising such rights. It also

imposes corresponding obligations on businesses to provide notices and disclosures regarding their information practices. This includes requiring businesses to provide consumers with clear and meaningful notices and disclosures that describe the categories of personal information collected, the purposes for which the information is used, whether it is sold or shared, the duration for which it will be retained, and how consumers may exercise their rights. These notices and disclosures must also include instructions for submitting requests and enabling consumers to make informed choices regarding the use of their personal information. To support these obligations, the CCPA directs the Agency to adopt rules ensuring that these requirements are communicated effectively to consumers. (See Civ. Code, §§ 1798.100–1798.135, 1798.185(a)-(b).) Accordingly, the Agency has promulgated regulations requiring that all disclosures and communications to consumers be easy to read and understand. (Cal. Code Regs., tit. 11, § 7003.)

The primary consumer-facing disclosure a business must provide is its privacy policy, which must include a comprehensive overview of a business’s information practices, both online and offline. It must clearly describe consumers’ rights under the CCPA and provide the necessary information for consumers to exercise those rights. In addition to the privacy policy, businesses are required to issue notices that inform consumers of specific rights, such as the right to opt-out of the sale or sharing of personal information, the right to limit the use of sensitive personal information, and the right to opt-out of Automated Decisionmaking Technology (ADMT) for significant decisions. (Cal. Code Regs., tit. 11, § 7011.)

In addition to the required notices and disclosures, the CCPA imposes limits on businesses’ collection, use, retention, and sharing of personal information through purpose limitation and data minimization principles. (Civ. Code, § 1798.100(c).) The regulations set out how businesses must operationalize these principles and explain how disclosures factor into consumers’ reasonable expectations about how businesses collect and handle their personal information. (Cal. Code Regs., tit. 11, § 7002.)

Friction In Exercising Privacy Rights

As noted above, the CCPA provides certain privacy rights to consumers; however, consumers must take action to exercise their rights.

The CCPA seeks to make it easy for consumers to exercise these rights and contains provisions to reduce friction consumers may experience when attempting to do so. For example, the CCPA prohibits businesses from requiring consumers to create accounts or to provide more information than necessary to direct a business not to sell or share their personal information or to limit the use and disclosure of sensitive personal information. (See Civ. Code, § 1798.135(c)(1).) The CCPA also directs the Agency to establish rules to help minimize burdens on consumers when exercising their privacy rights. (See Civ. Code, §§ 1798.185(a)(4)(A), (a)(6).) In addition, Agency-sponsored legislation (SB 923) was recently signed into law and takes effect January 1, 2027. It requires online-only businesses to provide an online method, such as a web form, for consumers to submit certain privacy requests, highlighting the importance of making it

easy for consumers to exercise their privacy rights.

The regulations currently impose requirements upon businesses related to how they provide consumers with privacy rights, and in certain instances more directly address friction. For example, the regulations prohibit businesses from adding unnecessary friction to the exercise of privacy rights, while providing guidance to businesses about how to give consumers easily accessible methods to submit their privacy requests and obtain their consent in ways that ensure they can make their choices freely. Making methods of submission more accessible and ensuring that consumers can make privacy choices freely are ways to reduce friction. The regulations also prohibit businesses from requiring consumers to verify their identity to opt-out of sale or sharing, to limit the use and disclosure of their sensitive personal information, or to opt-out of ADMT. The regulations prohibit businesses from requiring more information than necessary to process verifiable privacy requests. Minimizing the steps consumers must take and the information they must provide to exercise their privacy rights are also ways to reduce friction. (See Cal. Code Regs., tit. 11, §§ 7004, 7026(d), 7027(e), 7060, 7221(f).)

Both the Agency and the California Attorney General actively enforce the CCPA and the Agency's regulations. Their enforcement actions address business practices that create unnecessary friction for consumers. For example, the Agency's settlements with [Honda](#), [Todd Snyder](#), [Ford](#), [Tractor Supply](#), [PlayOn Sports](#), and [LocateSmarter](#) emphasize that businesses cannot require consumers to verify their identity to opt-out of sale or sharing, nor require more information than necessary to process privacy requests. These actions also underscore that businesses must provide consumers with effective means to opt-out of sale and sharing and recognize and honor opt-out preference signals. (The Agency's Board's enforcement decisions are posted at <https://privacy.ca.gov/about-us/board-decisions/>.)

Despite these efforts, consumers still struggle to navigate and understand notices and disclosures, and experience friction in exercising their privacy rights. Public feedback has identified ongoing harms, as well as potential solutions, that the informational session will highlight.

Informational Session Agenda

I. Usability Threats to Privacy Disclosures and Choice Interfaces

Dr. Lorrie Faith Cranor

Privacy policies are notoriously difficult for people to read and understand. In addition, privacy choice and consent interfaces also tend to be difficult for people to use and often leave people uncertain about the choices they have made. This session will highlight common threats to the usability of privacy disclosures and choice interfaces and suggest approaches to reducing friction and improving their usability.

II. Consumer Experiences with Privacy Requests and Notices

Matt Schwartz

CCPA provides consumers with a number of procedural rights and opportunities to review covered businesses' data processing activities. However, consumers are often frustrated by how these rights and notices are surfaced to them in practice. This session will review several of the common pain points and highlight how they can prevent from consumers fully leveraging their rights under the law.

III. A Practitioner's Perspective on Privacy Notices and Consumer Rights

David Stauss

This session will offer a practitioner's perspective on the pain points that privacy notices, cookie banners, and consumer rights requests create for both consumers and businesses. This session will propose practical solutions to these challenges and discuss long-term strategies for anticipating and addressing emerging issues.

IV. Friction & CCPA Rights Request Processes

Dr. Jennifer King

Despite prescriptive guidelines enshrined in the CCPA, California consumers can be stymied in their exercising of their data rights due to friction in the design of rights requests processes. Design friction consists of features that interfere with the completion of online tasks; at their most extreme they take the form of "dark patterns," interface designs that deceive or manipulate users into taking actions against their preferences. This talk will review design friction in CCPA rights requests processes by walking through real-world examples and discussing academic research that documents design friction and its impacts.

Speakers

Dr. Lorrie Faith Cranor is Director and Bosch Distinguished Professor in Security and Privacy Technologies of CyLab and FORE Systems University Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University. She also co-directs the Privacy Engineering program. Her research focuses on usable privacy and security, including empirical studies of privacy notice and choice mechanisms and privacy decision making. In 2016 she served as Chief Technologist at the US Federal Trade Commission. She founded the Symposium On Usable Privacy and Security (SOUPS) and co-founded the Conference on Privacy Engineering Practice and Respect (PEPR). She was elected to the ACM CHI Academy and named a fellow of ACM, IEEE, and AAAS. She received the ACM CHI Social Impact Award and Lifetime Research Award and the International Association of Privacy Professionals (IAPP) Privacy Leadership Award. She holds a doctorate in Engineering and Policy from Washington University in St. Louis..

Matt Schwartz is a Senior Policy Analyst at Consumer Reports, where he covers CR's legislative portfolio relating to privacy issues. He has played a leading role in advocating for strong, consumer-friendly privacy laws in states around the country, closely working with lawmakers in dozens of states to shape legislative proposals. His areas of focus include consumer data rights requests, data brokers, authorized agents, and ad-tech. Previously, he worked on technology policy and internet governance issues for ACT | The App Association and New America. He grew up in San Diego and received a B.A. in Political Science & International Affairs from Wake Forest University and an M.P.P. from Georgetown University's McCourt School of Public Policy.

David Stauss is a privacy attorney whose practice focuses on U.S. state and federal privacy law. His work spans comprehensive state privacy laws such as the CCPA, children's privacy and social media laws, data broker laws, biometric and health privacy laws, and AI laws and regulations. He is ranked by Chambers and is an IAPP Emeritus Fellow. For nearly a decade, David has advised state lawmakers across the country as an outside subject-matter expert on privacy, AI, and data breach legislation.

Dr. Jennifer King is the Privacy and Data Policy Fellow at the Stanford University Institute for Human-Centered Artificial Intelligence. An information scientist by training, Dr. King is a recognized expert in information privacy. Sitting at the intersection of human-computer interaction, law and policy, and the social sciences, her research examines the public's understanding and expectations of online privacy, the social impacts of technology design, and the policy implications of emerging technologies. Her current areas of research focus include AI and data policy, the use of consumer data for AI model training, regulating digital design, data broker compliance with the California Consumer Privacy Act, and manipulative algorithmic and interface design.