Yale Journal of Law & Technology
Volume 28, Symposium Issue

Governing Data: The Role of State Privacy Law

Jennifer M. Urban[1*]

Article Contents

Introduction **2**

The California Model: Constitutional Rights, Consumer Privacy Laws **7**

Enforcement 13

Data Brokers 17

Consumer Tools 19

Regulations 21

Strengthening Privacy and the Vital Role of States **27**

[1*] Clinical Professor of Law, University of California, Berkeley School of Law and Board Chairperson, California Privacy Protection Agency ("CPPA," Agency," and more recently, "CalPrivacy"). This talk, and resulting essay, represent my own views; nothing in it should be attributed to the Agency, its Board, or the University of California. While this essay discusses some of the CPPA's recent actions and official positions, any views I express about those actions and positions are solely my own. I am grateful to Professors Mihailis Diamantis and Rishab Nithyanand for the kind invitation, and to all the symposiasts for their thoughtful comments. It was an honor to open this important symposium and exciting to consider the valuable ideas contained within the symposium talks and papers. Thank you also to the fabulous team at the *Yale Journal of Law & Technology* for organizing everything so beautifully and providing expert editorial guidance. And thank you, for myself and for California, to the expert, mission-focused, and dedicated staff who make up the CPPA.

Introduction

Privacy is a fundamental right.[2]

I begin with this statement, which is both widely recognized as fact and heavily contested in its meaning. Certainly, it has been contested in practice, especially in recent decades, as data flows have arisen, grown to rivers, expanded to floods, and reshaped the economy. But we should not conflate the challenges that practical economic choices pose for fundamental rights—and that fundamental rights may pose for those who desire to collect, use, sell and share personal data—with the fundamental rights themselves.

Accordingly, if we take our given topic—"Governing Data"—literally, we should consider privacy a principal component of data governance. Relatedly, we should consider issues of "privacy" as compared to "data protection," and approaches to "informational privacy" (in data) in relation to autonomy and other fundamental interests as they are expressed in privacy protections.

With that in mind, I am going to discuss the role of state privacy law in data governance, focusing on California. That's partly because I am standing here as the Board Chairperson for the California Privacy Protection Agency,[3] and partly because I think California provides an illuminating example of policymakers', and the public's, ongoing tussles with the governance of personal data. Not only does California enshrine

---

[2] *This essay is based on the keynote talk I gave to open the Governing Data symposium on March 28, 2025. Just a few months later, some of the California activities I discussed developed significantly. Even more significantly, the role of states in protecting Americans' privacy—and giving them the tools to govern their data—has become critical in light of federal government activities, I have therefore updated certain examples and references, but the essay is still necessarily incomplete—federal efforts to access, use, combine, and disseminate Americans' most personal information continue.*

[3] As noted, however, I represent only my own views, and not the views of the CPPA or its Board.

the right to privacy in its state constitution, but it has also led the way in innovating privacy protections as data has become more and more economically and societally significant.

Why states? First, the states have taken the lead over the federal government in innovating effective privacy and data governance models. Nearly 20 states have passed generally applicable (as opposed to sectoral) consumer privacy laws in recent years, along with dozens of related laws, like the Illinois Biometric Information Privacy Act and the Colorado AI Act.[4] Second, unfortunately, states' efforts are critical to protecting privacy in light of recent federal attacks on data governance and privacy.

Briefly, some history of data-processing regulation. The idea that automated data processing—including by private entities—implicates due-process values has deep roots in the United States. Though concerns go back at least to the 1940s and still echo today,[5] a series of developments in the 1960s and 1970s brought attention to the effects of data gathering and use. In one important development, in the early 1970s, Former Secretary of Health, Education, and Welfare Elliot L. Richardson established an Advisory Committee on Automated Personal Data systems in response to "growing concern about the harmful consequences that uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens."[6] The Committee considered "changes in American

---

[4] ILL. BIOMETRIC PRIVACY INFO. ACT, 740 ILL. COMP. STAT. 14/ (2008)); (COLO. AI ACT, Colo. S. B. 25-205 (2024), *available at* https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf [https://perma.cc/F4HH-FE2U].

[5] *See* Hansi Lo Wang, *Some Japanese-Americans Wrongfully Imprisoned During WWII Oppose Census Question*, NPR.ORG (Dec. 26, 2018, 16:40 ET), https://www.npr.org/2018/12/26/636107892/some-japanese-americans-wrongfully-imprisoned-during-wwii-oppose-census-question [https://perma.cc/S4RD-GAXX].

[6] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS vii (1973),

society which may result from using computers to keep records about people."[7]

In 1973, the Committee published an influential report (the "Report") recommending the enactment of legislation establishing a "Code of Fair Information Practice"—expressed today as the "Fair Information Practice Principles" ("FIPPs")—for "automated personal data systems.[8] These principles, structured to reflect both process values (such as notice) and autonomy values (such as individual participation), proved highly influential and have since provided a basis for data privacy law and government policy both in the United States and internationally.[9]

Concerns about the automated processing of personal information coincided with public outrage in response to revelations of the Watergate scandal as well as the extensive government intelligence activities directed at Americans uncovered by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (commonly called the "Church Committee" after its chair, Frank Church).[10] In its comprehensive report, the Church Committee found that:

---

https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/3FEW-CJB6].

[7] *Id.*

[8] *Id.* at xx–xxiii.

[9] *See* U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974, 1-2 (2020), https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition [https://perma.cc/WPS8-QMJF]. For one 21st century example of how one U.S. agency has implemented the FIPPs, see Memorandum from the Chief. Priv. Off. of U.S. Dep't. of Homeland Sec., *Privacy Policy Guidance Memorandum: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, Memorandum No. 2008-01 (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/2024-01/Fair%20Information%20Principles_12_2008.pdf [https://perma.cc/FS6R-8VN3].

[10] *See generally* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTEL. ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: BOOK II — FINAL REPORT, S. REP. NO. 94-755 (Apr. 26, 1976).

> Intelligence agencies have collected vast amounts of information about the intimate details of citizens' lives and about their participation in legal and peaceful political activities. The targets of intelligence activity have included political adherents of the right and the left, ranging from activist to casual supporters. Investigations have been directed against proponents of racial causes and women's rights, outspoken apostles of nonviolence and racial harmony; establishment politicians; religious groups; and advocates of new lifestyles.[11]

These activities were shocking: wiretaps, bugging, mail-opening, infiltration of community meetings and even covert actions "designed to 'disrupt' and 'neutralize' domestic targets," including "domestic dissenters."[12] Activities went back decades and spanned presidential administrations from Franklin D. Roosevelt's to Richard Nixon's.[13] The purposes ranged from fear of Communist or Black nationalist infiltration, to a belief that peaceful dissident expression presaged violent acts, to powerful men's desire to punish their "enemies."

Congress, "facing a crisis of public trust" in the wake of the revelations, responded by passing the Privacy Act of 1974.[14] The Privacy Act, built on the FIPPs, has been the basis for federal government treatment of Americans' personal information since.

As noted, these same basic principles are at the center of privacy and data-protection laws throughout the world.[15] Over

---

[11] *Id.* at 58-65, 65.
[12] *Id.* at 7.
[13] *Id.* at 9-10.
[14] U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974, at 3 (2020), https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition [https://perma.cc/P7XD-QDHC].
[15] *See id.* at 1-2 (giving Europe's General Data Protection Regulation and the Organization for Economic Cooperation and Development's

time though, the United States diverged in significant ways from its counterparts abroad. Most notably, while other jurisdictions applied privacy protections to both public and private actors, there has been a sharp contrast in U.S. law between governmental use and use in the private marketplace. While the Privacy Act continues to govern federal governmental use of personal information, "consumers" in the private sector were left with a market-based, "notice-and-choice" approach.[16]

Although the concept of providing notice and offering a choice is loosely based on the FIPPs, much of the substance of the principles—such as minimizing data collection to what is necessary and offering data subjects the ability to participate meaningfully in decisions, was trimmed away in favor of a bare, two-step process: notice to the consumer via the (often lengthy and unclear) privacy policy or terms of service, and the consumer's choice to accept, or not.[17] Before the states became active, privacy enforcement in the U.S was centered in the Federal Trade Commission which, due to its consumer-protection-focused powers, generally considered the deceptiveness of privacy policies rather than whether the terms are fair.[18]

The due-process concept of "notice," then, became a rather limited concept. "Choice" did, too. "Choice" in the U.S. marketplace has generally meant a choice to interact with or use—or not—a company's products or services. Read the privacy policy. Find the terms acceptable, choose to use the company. Find the terms unacceptable, find a competitor with better terms. This approach persisted over decades.

Recently, however, bare "notice-and-choice" regimes have met with resistance from the American public and from lawmakers, especially in the states. Accordingly, I'll next focus

---

Guidelines on the Protection of Privacy and Transborder Data Flows as examples).

[16] *See* Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 261-62 (2014).

[17] NEIL RICHARDS, WHY PRIVACY MATTERS 174, 176 (2022).

[18] *See id*. (collecting sources).

on the recent development of state comprehensive consumer privacy laws in the U.S., centered on the protection of personal information in the marketplace, and starting in California. I will consider this through the lens of the very recent history of the first authority in the United States with full administrative authority based in that law—the California Privacy Protection Agency—and how the CPPA has approached its responsibilities and authority under the nation's first comprehensive consumer privacy law.

The California Model: Constitutional Rights, Consumer Privacy Laws

California—its government, its legislature, and its people—has long been a leader on data privacy in the United States. California's leadership dates back decades, at least dating to that mid-century moment of concern about computer processing and government overreach. Indeed, at that time, more than 50 years ago, a citizen initiative amended the California State Constitution to make explicit that [a]ll people are by nature" possessed of an "inalienable" right to privacy.[19]

Over the decades, California has continued to lead in the U.S., and to respond to the changing nature and practicalities of privacy threats, with the first data breach disclosure law, the first state law to require online privacy policies for commercial websites,[20] a strong medical privacy law,[21] additional

[19] RIGHT OF PRIVACY, Cal. Proposition 11, at 26 (1972), https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props [https://perma.cc/Q8CT-BQZM] ("This measure, if adopted, would revise the language of this section to list the right of privacy as one of the inalienable rights.") In full, Article I, Section 1 of the California Constitution now states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*." CAL. CONST. art. I, § 1 (emphasis added).

[20] Online Privacy Protection Act of 2003, 2003 Cal. Stat. 6183 (codified at CAL. BUS. & PROF. CODE §§ 22575-79).

[21] Confidentiality of Medical Information Act, 1981 Cal. Stat. 3040 (codified at CAL. CIV. CODE §§ 56-56.37).

protections for genetic information,[22] and protections for the privacy of digital book readers,[23] among others.

Until 2018, however, California's statutory laws were still basically sectoral. That changed in 2018, when the legislature—under pressure from a citizen initiative effort—adopted the California Consumer Privacy Act of 2018 ("CCPA").[24] The CCPA was the first comprehensive consumer privacy law passed in the United States.[25] It gives California "consumers"—that is, natural persons who are California residents[26]—rights over the personal information businesses collect about them. Specifically, the CCPA provides Californians with rights to access, delete, and opt out of the sale of their personal information.[27] Reciprocally, it requires businesses to inform consumers about how they collect, use, and retain personal information and effectuate their rights.[28]

Unlike older laws that focused protections on limited categories of "personally identifiable information" ("PII"), the CCPA's drafters recognized that attempts to define "PII" would always fall short of protecting privacy—privacy interests and harms aren't contained by predefined buckets of data.[29]

---

[22] Genetic Information Privacy Act, 2021 Cal. Stat. 4292 (codified at CAL. CIV. CODE §§ 56.18-56.186).

[23] Reader Privacy Act, 2011 Cal. Stat. 2906 (codified at CAL. CIV. CODE § 1798.90(i)-(k) (2024)).

[24] Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/76BC-3Q94]; California Consumer Privacy Act of 2018, 2018 Cal. Stat. 1807 (codified at CAL. CIV. CODE §§ 1798.100-1798.199.100 (2024)).

[25] Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 17:57 ET), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ [https://perma.cc/8FNG-U8MT].

[26] CAL. CIV. CODE §§ 1798.140(i).

[27] CAL. CIV. CODE §§ 1798.110–115 (rights to know and access), § 1798.105 (the right to delete), and § 1798.120 (the right to opt out of sale).

[28] *See, e.g.*, CAL. CIV. CODE § 1798.130 (notice and disclosure obligations to consumers).

[29] *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.

Accordingly, the CCPA protects "personal information," defined according to its connection with—and thus privacy implications for—a person or household. Specifically, "personal information" covered by the law is any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[30] This standard is illuminated (but not limited) by a long list of example types of information, including things that could be categorized as PII (such as name, address, and passport number) but also things like browsing or purchase history, geolocation, and employment information.[31] It specifically includes inferences made that create a profile about a person.[32]

The CCPA applies to "businesses," defined as the subset of for-profit California businesses that collect Californians' personal information and meet thresholds for revenue or for handling certain amounts of Californians' personal information.[33] Upon the CCPA's passage, some covered businesses immediately began lobbying the California legislature to weaken it.[34] In response, organizers developed a

---

REV. 1814, 1827-28 (explaining the risks of regulating based on too-rigid or too-expansive PII categories).

[30] CAL. CIV. CODE § 1798.140(v).

[31] CAL. CIV. CODE § 1798.140(v)(1)(A)-(L).

[32] CAL. CIV. CODE § 1798.140(v)(1)(K) (covering "[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes").

[33] An entity is a "business" covered by the CCPA if it meets any one of three thresholds: it has annual gross revenues of at least $25 million a year, adjusted for inflation (currently $26,250,000 annually); it buys, sells, or shares the personal information of at least 100,000 consumers or households annually; or it "derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information." CAL. CIV. CODE § 1798.140(d)(1)(A)-(C).

[34] Issie Lapowsky, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (Apr. 29, 2019, 3:09 PM), *https*://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/ [https://perma.cc/8U6L-Z3YS].

second citizen initiative, the California Privacy Rights Act ("CPRA"), that amended and extended the CCPA.[35] This initiative was placed directly before the voters, who approved it in November 2020.

The CPRA amendments buttressed and extended rights granted under the CCPA. First, they added a right to correct personal information held by a business, and a right to limit a business's use of "sensitive personal information" to the use necessary to perform a requested service.[36] Second, and importantly, the amendments also added or buttressed foundational autonomy concepts from the original, full set of FIPPs, and in some cases included mechanisms underpinned by data protection and consumer protection principles.

For example, drawing from the full FIPPs and from data protection principles, the amendments take the law even further from the bare "notice and choice" regime. For example, the purpose specification requirement was beefed up significantly to focus on *prior* purpose specification—not only must businesses specify the purposes for collecting personal information at the point of collection, but they cannot add any purposes that are incompatible with those already disclosed without again providing notice.[37]

Further, the initiative added meaningful data minimization concepts on top of the notice requirements. That is, a business can only collect, use, retain, or share personal information in ways that are "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is

---

[35] California Privacy Rights Act of 2020 (Prop. 24), 2020 Cal. Stat. 71 (amending CAL. CIV. CODE §§ 1798.100-1798.199.100 (2024)).

[36] CAL. CIV. CODE § 1798.106 (right to correct); CAL. CIV. CODE § 1798.121 (right to limit use and disclosure of sensitive personal information). The amendments also added a definition of "sensitive personal information." This covers especially revealing types of personal information, such as driver's license, passport, and financial account numbers; precise geolocation; protected identities like racial or ethnic origin, immigration status, and union membership; religious or philosophical beliefs; genetic and health data; and the like. CAL. CIV. CODE § 1798.140(ae).

[37] CAL. CIV. CODE § 1798.100(a)(1).

compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."[38] Whether the business's collection, use, retention, and/or sharing of the consumer's personal information is "reasonably necessary and proportionate," and whether a new purpose is compatible with the context understood by the consumer, are based on factors set out in regulations.[39] Regulations also clarify that the purposes for which the "personal information was collected or processed shall be consistent with the reasonable expectations of the consumer," and set out factors to determine whether this is the case.[40] These additions go beyond mere "choice" in the marketplace, embedding autonomy values.

The initiative also extended the CCPA to include concepts drawn from data protection and consumer protection models. For example, it added opt-out rights related to automated decisionmaking, as well as requirements that businesses do risk assessments if their processing of personal information poses a significant risk to consumers' privacy or security.[41] These echo

---

[38] CAL. CIV. CODE § 1798.100(c).

[39] Whether the handling is "reasonably necessary and proportionate" to the purpose is based on three factors: the minimum personal information that is necessary to achieve the business's purpose; the possible negative effects of the collection or process on the consumer; and whether there are additional safeguards to address the possible negative effects. CAL. CODE REGS. tit. 11, § 7002(d) (2024). Whether a new purpose is compatible with the context depends on three additional factors set out in regulations: the consumer's reasonable expectations about the purposes; the new purpose itself (including whether it is a business purpose); and the strength of the connection between these two factors. CAL. CODE REGS. tit. 11, § 7002(c) (2024). If there is a stronger link, then the new purpose is more likely to be compatible with the context in which the personal information was collected. CAL. CODE REGS. tit. 11, § 7002(c)(3) (2024).

[40] CAL. CODE REGS. tit. 11, § 7002(b) (2024). Understanding whether the purposes match the consumer's reasonable expectations depend on multiple factors, including: the consumer's relationship with the business; the type, nature, and amount of the personal information being collected or processed; and how apparent and explicit disclosures to the consumer are. CAL. CODE REGS. tit. 11, § 7002(b)(1)–(3) (2024).

[41] CAL. CIV. CODE § 1798.185(a)(15), § 1798.185(a)(14)(B).

longstanding European approaches to data protection, recently buttressed by the General Data Protection Regulation ("GDPR").[42] Both consumer protection and privacy autonomy principles are also reflected. For example, the initiative clarified that that purported consent obtained via "dark patterns" designed to "subvert or impair user autonomy" is not consent.[43]

To implement and enforce the law, the initiative established the California Privacy Protection Agency—the first agency in the United States with full administrative and enforcement authority that is focused on privacy.[44] Via the initiative, the voters gave the Agency the mission to "protect the fundamental privacy rights of natural persons" in California,[45] and tasked it with related responsibilities, including implementing and enforcing the CCPA, providing guidance to businesses, and educating the public about their rights under the law.[46]

The Agency, while still new, is now in full force. Its governing Board was appointed in March 2021, first met in June 2021, and brought the Agency into being during the course of that year. Today, the Agency has seven divisions. It is actively implementing and enforcing the CCPA, undertaking campaigns to enhance public awareness of privacy and help Californians exercise their rights, and advising on legislative and policy activity within its expertise.

I will focus on some recent Agency activities that illustrate some of the key mechanisms in the CCPA to create meaningful choice, and some of the mechanisms that echo data protection and consumer protection principles.

---

[42] Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119/1) 1 (EU) [hereinafter GDPR].

[43] CAL. CIV. CODE § 1798.140(l) (defining "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice[.]"); CAL. CIV. CODE § 1798.140(h) (excluding "agreement obtained through the use of dark patterns" from the definition of "consent").

[44] CAL. CIV. CODE §§ 1798.199.10(a).

[45] CAL. CIV. CODE §§ 1798.199.40(c).

[46] CAL. CIV. CODE §§ 1798.199.40(a)-(f).

Enforcement

I'll start with the most recent development: enforcement. The California Attorney General's Office and the CPPA share enforcement authority for the CCPA. The CPPA's authority to enforce the CCPA took effect in July 2023. Since then, the enforcement division has grown from just the head of enforcement to a full Enforcement Division representing decades of diverse experience, including former prosecutors, in-house privacy counsel, litigators from large law firms, and the former Chief Privacy Officer of a large tech company, as well as growing technical expertise.

The Agency's enforcement work fulfills multiple goals. In addition to directly enforcing the law, it serves to guide businesses and enhance public understanding through its actions and decisions. I'll provide three examples: enforcement advisories, sweeps, and final decisions (which often take the form of public settlements).

First, advisories. Enforcement advisories share observations with the regulated community to offer information and support businesses' compliance efforts.[47] The Agency announced two advisories in 2024. One advisory stresses the importance of avoiding misleading or manipulative "dark patterns," thus emphasizing the importance of consumer protection, individual autonomy and dignity, and meaningful choice.[48] The other advisory provides information about applying data minimization to consumer requests.[49] This is key

---

[47] *Resources: Enforcement Advisories*, CAL. PRIV. PROT. AGENCY (last visited Oct. 19, 2025), https://cppa.ca.gov/resources.html [https://perma.cc/39LF-AG8Q] ("The Agency's Enforcement Division issues advisories to share observations with the regulated community and encourage compliance with the CCPA.").

[48] CAL. PRIV. PROT. AGENCY, ENFORCEMENT ADVISORY NO. 2024-02: AVOIDING DARK PATTERNS: CLEAR AND UNDERSTANDABLE LANGUAGE, SYMMETRY IN CHOICE (Sept. 4, 2024), https://cppa.ca.gov/pdf/enfadvisory202402.pdf [https://perma.cc/RZX2-QRAP].

[49] CAL. PRIV. PROT. AGENCY, ENFORCEMENT ADVISORY NO.2024-01: APPLYING DATA MINIMIZATION TO CONSUMER REQUESTS (Apr. 2, 2024),

for businesses implementing data minimization in California—while, as noted, data minimization principles are very much part of the full, original FIPPs, they are more commonly seen implemented in data-protection law.

Second, sweeps. Enforcement sweep announcements make businesses aware that the Agency is taking a close look at specific industries or practices. As soon as its enforcement power took effect in July 2023, the Agency announced an enforcement sweep on the review of privacy practices of connected vehicles and related technologies.[50] Data practices in the vehicle industry are crucially important to consumer privacy because connected vehicles typically gather large amounts of revealing information about individual and household habits, including locations, preferences for music and other entertainment, and daily routines.[51] Since then, it has announced additional sweeps, including one undertaken jointly with authorities in Colorado and Connecticut, and one focused on data brokers.[52]

I'll highlight three final decisions, which provide a record of the Agency's reasoning in applying the law and act as guidance documents to help both covered businesses and the public understand and implement the law. Final decisions are the end result of the administrative process, and are made by the Board

---

https://cppa.ca.gov/pdf/enfadvisory202401.pdf [https://perma.cc/7TAL-U2KQ].

[50] Announcement, Cal. Priv. Prot. Agency, CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies (July 31, 2023), https://cppa.ca.gov/announcements/2023/20230731.html [https://perma.cc/H2RV-PD5C].

[51] *Id.*

[52] Announcement, *California Privacy Protection Agency Announces Joint Investigative Privacy Sweep: CA, CO, and CT Investigate Businesses Refusing to Honor Consumers' Right to Opt-Out of the Sale of Their Personal Information*, CAL. PRIV. PROT. AGENCY (Sept. 5, 2025), https://cppa.ca.gov/announcements/2025/20250909.html [https://perma.cc/ADA7-366M]; Announcement, *CPPA's Enforcement Division to Review Data Broker Compliance with the Delete Act*, CAL. PRIV. PROT. AGENCY (Oct. 30, 2024) [hereinafter *Data Broker Compliance*], https://cppa.ca.gov/announcements/2024/20241030.html [https://perma.cc/ER97-MK7Z].

of the Agency on a full review of the case. (The Board is the adjudicative body, so we are siloed off from the enforcement division's investigative efforts and consider the proposed decision or settlement at the end of the process.)

When we met in 2025 for the symposium, the Board had just considered the Agency's first final CCPA case. Keeping with the theme of connected cars, the Board approved a settlement between the CPPA and Honda for Honda's privacy violations under the CCPA.[53] At issue was that Honda made it difficult for consumers to manage their privacy preferences for connected vehicles. This resulted in Honda having to pay a fine of $632,500 and—importantly—change its business practices.[54]

The settlement enforces data minimization requirements, notably the principle of necessity. Honda required consumers to provide excessive personal information before they could opt-out of the sale and sharing of their data. For example, though it needed only two data points to process an opt-out, Honda required consumers to fill out eight separate fields with information.[55] Thus, it was collecting notably more personal information than necessary to execute the opt-out request.[56]

The settlement also reflects the autonomy and consumer protection principles embedded in the law. For example, Honda failed to provide symmetry in choice—exercising the privacy-protective option of turning off advertising cookies (which were initially turned on) required a consumer to take more steps than opting back in did.[57] This was a form of "dark pattern" that undermined consumer choice and autonomy.

Honda also shared consumer data with advertising technology companies without being able to show that the

---

[53] Am. Honda Motor Co., Inc., Case No. ENF23-V-HO-2, (Cal. Priv. Prot. Agency Mar. 7, 2025), at 12-13 https://cppa.ca.gov/regulations/pdf/20250307_hmc_order.pdf [https://perma.cc/KB7U-689C].

[54] *Id.*

[55] *Id.* at 4-6.

[56] *Id.*

[57] *Id.* at 8-10.

proper agreements were in place.[58] The CCPA requires agreements with third parties to identify the limited purposes for using personal information and restricting the third party's use to only those purposes—and agreements must require the third party to abide by the CCPA and provide the same level of protection as businesses covered by the CCPA.[59] Processing is not prohibited by default, as it is in Europe,[60] but the CCPA's contractual requirements are intended to prevent rights from being circumvented with data-sharing agreements. Honda was unable to produce the necessary agreements.[61]

As part of the resolution of the case, Honda was required to fix these and other deficits in its practices.[62] Importantly, it is required to simplify how consumers exercise their rights and ensure proper safeguards are in place when sharing data with third parties. Thus, a key aspect of this settlement is that Honda agreed, not just to pay a fine, but to change its business practices—and to change them so that consumers can make meaningful choices about their personal information.

Indeed, the Honda case represents the first CCPA enforcement action to incorporate UX (user-interface design) requirements. It requires Honda to undertake a UX design evaluation, including A/B testing, to ensure that the methods for consumer requests are easy to use and avoid elements that confuse consumers.[63]

As the Honda case shows, the Agency's enforcement division will seek remedies that change business practices where needed. (Since I gave this talk, the Agency has resolved additional cases under the CCPA that emphasize business

---

[58] *Id.* at 10-11.

[59] *See* CAL. CIV. CODE §§ 1798.100(d); CAL. CODE REGS. tit. 11, §§ 7051, 7053.

[60] *See, e.g.*, Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1747 (2021).

[61] Am. Honda Motor Co., Inc., Case No. ENF23-V-HO-2 (Cal. Priv. Prot. Agency Mar. 7, 2025), at 10 para. 69, https://cppa.ca.gov/regulations/pdf/20250307_hmc_order.pdf [https://perma.cc/KB7U-689C].

[62] *Id.* at 12-13.

[63] *Id.* at 13 para. 79.

practices. Among other points, recent cases emphasize that businesses are responsible for failures of third-party services they use to handle personal information,[64] and that employees and job applicants are protected under the CCPA.[65])

Data Brokers

The Agency's recent actions against data brokers—which buy, sell, and share consumer information without having a direct relationship to the consumer—also provide notable examples. These cases stem from another recent California law: in 2023, the California legislature passed the Delete Act, a law that strengthened consumers' privacy protections with respect to data brokers, and tasked the CPPA with implementing and enforcing it.[66]

The Delete Act took effect in January 2024, and later that year the Agency announced a sweep related to data broker compliance with the law.[67] Since then, the Board has reviewed and approved eight Enforcement Division actions against data brokers. I'll highlight two notable settlements we've reached this year.

The first case I'll highlight was against a Florida-based broker called National Public Data. The CPPA fined National Public Data for failing to register as a data broker with the Agency.[68] If that name sounds familiar, it's likely because the company made national news for a major data breach in 2024 that exposed the personal information in billions of records,

---

[64] Todd Snyder, Inc. Case No. ENF23-M-TO-26 (Cal. Priv. Prot. Agency May 1, 2025), https://cppa.ca.gov/pdf/20250501_snyder_order.pdf [https://perma.cc/V28C-AJAB].

[65] Tractor Supply Co., Case No. ENF24-M-TR-04, (Cal. Priv. Prot. Agency Sept. 26, 2025), https://cppa.ca.gov/pdf/20250930_tractor_supply_bd_sfo.pdf [https://perma.cc/Y696-SDMK].

[66] Cal. Delete Act, CAL. CIV. CODE §§ 1798.99.80–1798.99.89 (2024).

[67] *See Data Broker Compliance*, *supra* note 52.

[68] Jerico Pictures, Inc., d/b/a Nat'l Pub. Data and RecordsCheck.net, Case No. ENF24-D-JE-16, (Cal. Privacy Prot. Agency, May 2, 2025).

affecting around 300 million individuals.[69] This case shows the profound effect one business can have on the privacy of millions of people.

The second case was against Background Alert, Inc., a "people search" site which promoted its ability to dig up "scary" amounts of information about people. The company failed to register with the CPPA as a data broker. As part of the resolution, the company agreed to cease operations through 2028 or face a $50,000 penalty.[70]

The case against Background Alert, Inc. is especially notable because it underscores the fact that *inferences* are protected personal information under the CCPA and the Delete Act when they are used to create profiles about consumers. In response to customers' search requests, Background Alert searched what it claimed to be "literally billions" of public records, such as birth records, death records, marriage and divorce records, professional licenses, and registered sex offender records.[71]

Though in many circumstances public records themselves may fall outside of the CCPA's definition of protected "personal information" as "publicly available" data,[72] Background Alert advertised that it then looked for patterns in the data about the person being searched, including looking for "who may somehow be associated with" the search subject and "track[ing] down any alarming patterns they may have."[73]

---

[69] Zack Whittaker, *National Public Data, The Hacked Data Broker That Lost Millions of Social Security Numbers and More, Files for Bankruptcy*, TECHCRUNCH (Oct. 14, 2024) https://techcrunch.com/2024/10/14/national-public-data-the-hacked-data-broker-that-lost-millions-of-social-security-numbers-and-more-files-for-bankruptcy/ [https://perma.cc/N2AV-N4DV].

[70] Background Alert, Inc., Case No. ENF24-D-BA-23 (Cal. Priv. Prot. Agency, Feb. 26, 2025), https://cppa.ca.gov/pdf/settlement_background_alert.pdf [https://perma.cc/U78C-Z3AE].

[71] *Id.* at 3 para. 21-22.

[72] *See* CAL. CIV. CODE § 1798.140(v)(2); CAL. CIV. CODE § 1798.99.80(a).

[73] Background Alert, Inc., Case No. ENF24-D-BA-23 (Cal. Priv. Prot. Agency, Feb. 26, 2025), at 4-5,

These connections constituted inferences, which separately qualify as personal information and thus are covered by the CCPA and the Delete Act.[74] As the case points out, inferences pose "special risks to privacy," as they can use "seemingly innocuous data points" to infer deeply personal information about people, such as whether they are "gun owners, immigrants, members of faith communities, veterans, and patients at reproductive healthcare facilities."[75]

Consumer Tools

One theme of the Enforcement Division's work is ensuring that businesses are moving beyond "notice and choice" to provide meaningful, actionable, timely choice that consumers can realistically make. I'm excited by two additional examples of innovative California policy that further implements these goals.

Continuing with data brokers, the Delete Act is providing tools that consumers can use to learn where their data might be and assert their rights to delete it. Because data brokers do not have a direct relationship with consumers,[76] the first challenge is for consumers to find them. Thus, the Delete Act mandates that data brokers register with the CPPA, and that the CPPA maintain a website that provides the registry information to the public.[77] Recent updates to the law also require that data brokers disclose certain types of that they collect, so that consumers and other stakeholders can quickly search for brokers that hold that kind of data.[78] Data brokers must disclose that they collect, for example, the personal information of minors, consumers' precise geolocation, and

---

https://cppa.ca.gov/pdf/settlement_background_alert.pdf [https://perma.cc/U78C-Z3AE].

[74] *See* CAL. CIV. CODE § 1798.140(v)(2); CAL. CIV. CODE § 1798.99.80(a).

[75] Background Alert, Inc., Case No. ENF24-D-BA-23 (Cal. Priv. Prot. Agency, Feb. 26, 2025), at 5, para. 26-30, https://cppa.ca.gov/pdf/settlement_background_alert.pdf [https://perma.cc/U78C-Z3AE].

[76] CAL. CIV. CODE § 1798.99.80(a).

[77] CAL. CIV. CODE §§ 1798.99.82(a), 1798.99.84.

[78] CAL. CIV. CODE § 1798.99.82(a)(2)(B)-(E).

reproductive health care data.[79]

The Delete Act was further improved last year to provide tools to help consumers request that data brokers delete their personal information from data brokers registered with the state via a one-stop shop instead of requiring consumers to make hundreds of individual requests. Namely, 2024 amendments to the Act mandated that the Agency build an "accessible deletion mechanism" to provide that clearinghouse to California residents.[80] The Agency has now built the mechanism—which it is calling the "DROP system" (for "Delete Request and Opt–Out Platform")—and launched it on January 1, 2026.[81]

The DROP is a first-of-its-kind tool. Californians are able to access the platform through the Agency and direct some, or all, registered data brokers to delete their personal information in a single request.[82] Data brokers for their part, must begin accessing the platform in August, 2026 to retrieve deletion requests; thereafter, they must continue retrieving requests and removing newly collected data every 45 days.[83] Data brokers will report the status of each request to the Agency, indicating whether the data was deleted, opted out, or deemed subject to an exemption.[84] By creating this one-stop shop for finding and deleting personal information held by data brokers, the DROP promises to greatly improve consumers' ability to effectuate

---

[79] CAL. CIV. CODE § 1798.99.82(a)(2)(B)-(E).

[80] CAL. CIV. CODE § 1798.99.86.

[81] *Proposed Regulations on Accessible Deletion Mechanism – Delete Request and Opt–out Platform ("DROP") System Requirements,* CAL. PRIV. PROT. AGENCY, (last visited Oct. 22, 2025), https://cppa.ca.gov/regulations/drop.html [https://perma.cc/VE6M-TFWM] (providing information about the process for finalizing regulations to implement the DROP, as well as the current draft regulations). The DROP tool is available to California residents at https://privacy.ca.gov/drop/.

[82] CAL. CIV. CODE § 1798.99.86(a)-(b).

[83] CAL. CIV. CODE § 1798.99.86(c).

[84] Modified Text of Proposed Regulations: Data Broker Registration and Accessible Deletion Mechanism § 7614 (Cal. Priv. Prot. Agency Jul. 31, 2025), https://cppa.ca.gov/regulations/pdf/20250731_modified_text.pdf [https://perma.cc/PDJ3-MR69].

their privacy rights.

Since the conference, California has buttressed another important tool for consumers: opt-out preference signals ("OOPS"). These are settings that consumers can set in browsers, which then automatically signal to businesses that consumers are opting out of sale or sharing. The CCPA already requires businesses to honor these signals. But browser providers haven't previously been required to provide an OOPS setting. Now they are. A CPPA-supported bill to require browsers to offer the OOPS option was passed this fall and has been signed by the Governor.[85]

Both of these innovations harness technology to improve consumers' ability to exercise their rights at scale—in a manner that's more commensurate with how personal information is collected, used, and shared today. They will help make exercising rights truly actionable for consumers.

Regulations

As I noted, the CCPA is responsible for both enforcing and implementing the law. Indeed, the 2020 initiative that created the CPPA tasked the new Agency with a long list of specific rulemaking responsibilities to implement the law.[86] Accordingly, a major function of the Agency since its inception has been implementing the law through regulations. These included additional regulations and updated regulations to implement opt-outs, deletion rights, the new correction right, and updates to notices and responses by businesses.[87]

Mandated rulemaking also included data-protection-like privacy and security risk assessments and consumer rights

---

[85] *See* Cal. Opt Me Out Act, A.B. 566 (to be codified at CAL. CIV. CODE § 1798.236); Announcement, *Protect Their Personal Data*, CAL. PRIV. PROT. AGENCY (Oct. 8, 2025), https://cppa.ca.gov/announcements/2025/20251008_2.html [https://perma.cc/Y5GY-QQPB].

[86] *See* CAL. CIV. CODE § 1798.185 for the complete list.

[87] CAL. CODE REGS. tit. 11 (Cal Privacy Prot. Agency Mar. 29, 2023), https://cppa.ca.gov/regulations/pdf/20230329_final_regs_text.pdf [https://perma.cc/3X6V-UQF5].

related to automated decisionmaking.[88] In a development since the March symposium, the Agency has now completed regulations on these topics as well, thus completing all of the rulemaking initially mandated by the initiative.[89] These new rights for consumers and responsibilities for businesses significantly move the needle for U.S. privacy law. I'll give a brief overview of these topics and discuss the automated decisionmaking regulations as an example.

The CCPA, as amended by the citizen initiative, required the Agency to issue regulations on several interrelated requirements. First, the Agency was to issue regulations requiring "businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security" undertake annual cybersecurity audits and to prepare risk assessments covering their processing of personal information.[90] Importantly, the statute explicitly states that businesses must weigh the benefits and risks of processing and prepare risks assessments "with the goal of *restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing* to the consumer, the business, other stakeholders, and the public."[91] This requirement echoes similar requirements, such as the Data Protection Impact Assessments required in Europe[92] and similar assessments under United States federal law.[93]

The initiative amendments imposed an additional

---

[88] CAL. CIV. CODE § 1798.185(a)(14)-(15).

[89] *California Finalizes Regulations to Strengthen Consumers' Privacy*, CAL. PRIV. PROT. AGENCY (Sept. 23, 2025), https://cppa.ca.gov/announcements/2025/20250923.html [https://perma.cc/HH52-JH87].

[90] CAL. CIV. CODE § 1798.185(a)(14).

[91] CAL. CIV. CODE § 1798.185(a)(14)(B) (emphasis added).

[92] *See Data Protection Impact Assessment (DPIA)*, EUR. DATA PROT. SUPERVISOR (last visited Oct. 19, 2025), https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en [https://perma.cc/M6M4-9GHV]. DPIAs are required, for example, by the GDPR. Commission Regulation 2016/679, 2016 O.J. (L 119/1) 1 (EU) [hereinafter GDPR], at art. 35.

[93] *See, e.g.*, E-GOVERNMENT ACT OF 2002, Pub.L. 107–347 § 208, 116 Stat. 2921–23 (Dec. 17, 2002).

requirement that charges the CPPA with issuing regulations that implement "access" and "opt-out" rights for consumers "with respect to businesses' processing of personal information in their use of automated decisionmaking technology, including profiling."[94] In this instance, the right to access requires "businesses' response to access requests to include meaningful information about the logic involved in the decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer."[95]

For those who follow data protection law, the echoes of GDPR Article 22—which limits processing for automated decision-making, including profiling, and Article 15, regarding the need to provide "meaningful information about the logic involved"—will be easy to hear.[96]

Such requirements were entirely new to the United States, however. The required regulations were thus especially necessary to implement the statute's requirements. The Agency therefore engaged in an especially robust rulemaking process—spanning, in the end, four full years of pre-rulemaking fact-finding and public comment, discussion of draft language, and the formal rulemaking itself.[97] The staff and Board considered thousands of pages of written comments, several days of public hearings and other public comment, and sources ranging from original research on related topics to approaches taken in other jurisdictions.[98]

This collaborative process was resource-intensive, but necessitated by the newness of the law and the need to make the requirements executable for businesses and meaningful for consumers. For example, I quoted the statute in its entirety on

---

[94] CAL. CIV. CODE § 1798.185(a)(15).
[95] CAL. CIV. CODE § 1798.185(a)(15).
[96] *See* GDPR at arts. 15, 22.
[97] *See CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Regulations*, CAL. PRIV. PROT. AGENCY (last visited Oct. 19, 2025), https://cppa.ca.gov/regulations/ccpa_updates.html [https://perma.cc/KT9T-C5V6] (documenting the rulemaking record and collecting materials).
[98] *See id.*

the point of rights related to automated decisionmaking. That is, "automated decisionmaking technology" was not defined—it was up to the Agency to define it. Similarly, the Agency was charged with implementing the rights of access and opt-out, which were not specified in detail in the statute, in regulations.

When we met at the symposium, I explained that that the Agency was engaged in the formal rulemaking process. Since then, the regulations were further revised via that process, presented for another round of public comment, formally approved by the Board, and approved by California's Office of Administrative Law.[99] The regulations took effect as law in California on January 1, 2026,[100] making California the first jurisdiction in the United States to implement an opt-out right for automated decisions.

The final regulations[101] balance the need to create meaningful rights for Californians in a rapidly intensifying area of data processing together with the need for the law to be implementable by businesses.

As implemented by the new regulations, Californians have rights of opt-out and access with respect to automated decisionmaking technology ("ADMT") defined as "any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking."[102] This includes, as required by the statute, profiling of consumers that fits these

---

[99] Cal. Off. Admin. Law, Notice of Approval of Regulatory Action, In re Cal. Priv. Prot. Agency (Sept. 22, 2025), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_noa.pdf [https://perma.cc/8JDM-5B3J].

[100] *Id*.

[101] Cal. Consumer Privacy Act Regulations (Cal Priv. Prot. Agency, effective date Jan. 1, 2026), https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf [https://perma.cc/AB83-4XWB] (to be codified at CAL. CODE REGS. tit. 11).

[102] *See* Cal. Consumer Privacy Act Regulations, § 7001(e) (Cal Priv. Prot. Agency, effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

characteristics.[103] (Profiling is automated processing that is used to evaluate a natural person's personal characteristics, such as intelligence and predispositions, in particular to analyze or make predictions about the person's work performance, health, economic situation, behavior and other characteristics.[104])

These rights apply for "significant decisions" made with ADMT. These include decisions that have notable effects on consumers' lives, for example, decisions about lending, employment, education, housing.[105] When a business uses an ADMT for a significant decision, it must provide consumers with a Pre-use Notice that informs them that the business is using ADMT and that they have the right to access information about the ADMT and the business's use of it, as well as the right to opt out of the business's use of ADMT to make the significant decision.

Should the consumer choose to exercise their right to access information, the business has to explain the specific purpose for which it wishes to use the ADMT in relation to the consumer.[106] It also must provide information about the logic of the ADMT that enables the consumer to understand how outputs—related specifically to the consumer—are generated based on their personal information, the outcome of the decision for the consumer, and how the ADMT factored into

---

[103] CAL. CIV. CODE § 1798.185(a)(15); s*ee also* Cal. Consumer Privacy Act Regulations, § 7001(e)(2) (approved Sept. 22, 2025; effective date Jan. 1, 2026) (last visited Oct. 19, 2025) (to be codified at CAL. CODE REGS. tit. 11).

[104] *See* Cal. Consumer Privacy Act Regulations, § 7001(ii) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

[105] *See* Cal. Consumer Privacy Act Regulations, § 7001(ddd) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (last visited Oct. 19, 2025) (to be codified at CAL. CODE REGS. tit. 11).

[106] *See* Cal. Consumer Privacy Act Regulations, § 7222(b) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

the decisionmaking process.[107] The business must provide this information for each significant decision it would like to make about the consumer using ADMT.[108]

The consumer also has the right to opt out of the business's use of ADMT for many significant decisions.[109] The business has to provide at least two methods for opt-out, and must use methods that make opting out "easy for consumers to execute" and that "require minimal steps."[110] There is an exception: human-reviewed appeals. A business does not have to provide an opt-out to consumers if it instead provides an appeal to a human reviewer with the authority to overturn the ADMT decision.[111] To qualify, the appeals method has to meet certain requirements to ensure that it is a genuine review of the decision—not window-dressing—that provides a true appeal of the ADMT decision for the consumer.[112]

I won't say much about the new regulations related to privacy and security risk assessments, but note that businesses that intend to process consumers' personal information to train ADMTs or to use them for significant decisions must conduct risk assessments that consider those activities before

---

[107] *See* Cal. Consumer Privacy Act Regulations, § 7222(b)(2)-(3) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (last visited Oct. 19, 2025) (to be codified at CAL. CODE REGS. tit. 11).

[108] *See* Cal. Consumer Privacy Act Regulations, § 7222(b)(3)(A) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (last visited Oct. 19, 2025) (to be codified at CAL. CODE REGS. tit. 11).

[109] *See* Cal. Consumer Privacy Act Regulations, § 7221 (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

[110] Cal. Consumer Privacy Act Regulations, § 7221(e) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

[111] *See* Cal. Consumer Privacy Act Regulations, § 7221(b)(1) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

[112] *See* Cal. Consumer Privacy Act Regulations, § 7221(b)(1)(A)–(B) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

commencing.[113]

Automated decisionmaking is here to stay, but the CCPA, as amended, and now as implemented in regulations, provides consumers with some transparency and choice regarding its use in their lives. And as with other aspects of the California law, these requirements include notice-and-choice elements, enhanced to make them actionable for consumers. At the same time, autonomy values and data protection concepts are embedded in consumers' right to reject automated decisions that significantly affect them, and in the requirements for prospective risk assessments.

Strengthening Privacy and the Vital Role of States

Indeed, this framework undergirds all of the examples I've given. California has melded an updated notice-and-choice framework—made tangible, with stated rights that can be exercised, meaningful notice, and actionable mechanisms for choice—with data protection and autonomy principles. These are consequential changes.

I don't mean to overstate the connections here. As I noted earlier, in Europe, for example, the underlying default is to disallow processing without an approved reason.[114] In the United Sates, the default is still processing.

That bears repeating: in the U.S., the default is still processing.

Similarly, while it is agreed that privacy is a fundamental right—clearly identified as such in California, and in the EU Charter of Human Rights—this does not provide us with a ready-made approach, especially when the defaults in each jurisdiction contrast so sharply. Embedding this concept in policymaking is key to developing policy that reflects the true

---

[113] *See* Cal. Consumer Privacy Act Regulations, § 7150(b)(3), (6) (Cal Priv. Prot. Agency, approved Sept. 22, 2025; effective date Jan. 1, 2026) (to be codified at CAL. CODE REGS. tit. 11).

[114] Commission Regulation 2016/679, 2016 O.J. (L 119/1) 1 (EU) [hereinafter GDPR], at art 6. *See also* Chander, Kaminski & McGeveran, *supra* note 60, at 1747 (collecting sources).

stakes. As my former CPPA Board colleague Lydia de la Torre has explained, in Europe, vindicating privacy *rights* requires showing harm. For *data protection*, as she puts it, the automated processing *is* the harm. The U.S. doesn't have a tidy taxonomy to apply here, and continues to tussle with concepts of harm in privacy cases.[115]

All comparative work must recognize the effects of these differences.

Still, while it's important not to overstate the connections between more substantive models of privacy regulation and California's, it's also important not to understate them, or to ignore the trend toward more robust approaches. I emphasized the long process required to develop California's recent regulations to illustrate the importance of a broad-based and detailed public discussion to ground new policies, but also for a related reason: a lot has happened with regard to privacy and data protection law in the past five years (since the 2020 initiative), four-and-a-half years (since the Board was appointed and the agency could begin to develop), and four years (since we began work on the regulations I mentioned). While the approaches taken by the United States and Europe diverged years ago and have not fully reconnected, recent efforts made by California and other U.S. states do hark back to broader principles drawn from felt concerns about information databases and computer processing that developed through the 1960s and found purchase in the 1970s in both the U.S. and Europe.

Today's increased activity initially came in reaction to the accelerating use of personal data throughout the economy.

---

[115] *See generally* TransUnion LLC v. Ramirez, 594 U.S. 413 (2021); Spokeo v. Robins, 578 U.S. 330 (2016). *See also* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) (discussing the current incoherence of harm in United States privacy law and proposing a typology of privacy harms and guidance for when harm should matter in privacy cases). Indeed, "tussle" may be an optimistic descriptor of the situation. Professors Citron and Solove begin their exploration of "harm" in U.S. privacy law thusly: it "has become one of the biggest challenges in privacy law" and "a jumbled, incoherent mess" addressed by courts "inconsistently and with considerable disarray." *Id*. at 796.

We've had waves of personal-information-intensive business models. To name just a few: social media; "Big Data;" the "Internet of Things;" and "smart" everything. There was attention to each of these, but we in the U.S. did not get sustained policymaker attention to comprehensive models of privacy law until California's law, in 2018.

Since then, attention to privacy has exploded, and has only accelerated since ChatGPT was released in November 2022. The advent of "AI" has prompted numerous policy questions and responses, but privacy in the governance of AI systems is certainly a main theme. California's Assembly Bill 1008 emphasized this. A.B. 1008, which Governor Gavin Newsom signed into law in the fall of 2024, underscores that personal information under the CCPA includes information that exists in AI systems.[116] Colorado has passed a similar law—the Colorado Artificial Intelligence Act, which took effect in February 2026. It also echoes data protection concepts, centering on "high-risk artificial intelligence systems" that make or are "a substantial factor in making" a "consequential decision."[117] The National Conference of State Legislatures documented hundreds of "AI-related" bills—not including bills "related solely to specific AI technologies, such as facial recognition, deepfakes, or autonomous vehicles—introduced in state legislatures in the 2025 session (as of July).[118]

Ultimately, we find ourselves in an active moment of change. In the time since California passed the CCPA, eighteen other states have enacted consumer-data privacy laws of varying degrees of protection.[119] After years of inaction,

---

[116] Cal. A.B. 1008, (Sept. 28, 2024) (codified at CAL. CIV. CODE § 1798.140(v)(4)(C)), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1008 [https://perma.cc/6X3J-TZ9E].

[117] COLO. AI ACT, Colo. S. B. 25-205, § 6-1-1701(9) (2024).

[118] *Artificial Intelligence 2025 Legislation*, NATL. CONFERENCE OF STATE LEGISLATURES (July 10, 2025), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation [https://perma.cc/K9UY-6V7G].

[119] U.S. STATE PRIVACY LEGISLATION TRACKER 2025: COMPREHENSIVE CONSUMER PRIVACY BILLS, IAPP, (Oct. 10, 2025),

Congress has introduced consumer privacy legislation twice—even incorporating principles like data minimization. Unfortunately, however, these bills moved to undermine state efforts with broad preemption provisions.

This flurry of activity brings us directly to the question for this conference—what does governing data actually entail? What should it entail?

Here, I reemphasize that I am speaking only for myself and not for the CPPA or the CPPA Board. My view is that data governance must take into account, take seriously—and indeed, center—individual privacy. The longstanding inadequacy of U.S. privacy law stemmed from the fact that historical concerns about data regarding natural persons were not adequately addressed as time and technology moved forward. In today's world, the concerns about computer processing that arose in the 1960s and 1970s have accelerated even as policy remains behind. And where those concerns, in the United States, focused most closely on governmental collection and use of data, we now know that the porosity between commercial and government collection and use necessitates attention to both.

California and other states have picked up the baton. But we must grapple deeply with these questions in the face of accelerating technological, economic, and governmental change.

And then—not least—there is the world prior to January 20, 2025, and the world after. The 2025 inauguration coincided with or was quickly by followed actions that threaten to upend entirely the foundation of privacy and data protection that, at the federal level, has been in place since the 1970s, and in some cases approaching a century.

On the day of his second inauguration, President Trump issued Executive Order 14158 establishing the Department of Government Efficiency ("DOGE").[120] The DOGE EO directs

---

https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/9BWN-VQ5N].

[120] Exec. Order No. 14158, 90 C.F.R. 8441, § 1 (Jan. 20, 2025).

Agency Heads to grant DOGE full access to "all unclassified agency records, software systems, and IT systems."

And just before this symposium was held, the Trump Administration issued Executive Order 14243, "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos.[121] This "Information Silos EO" directs agencies to take steps needed, to ensure "full and prompt access to all unclassified agency records, data, software systems, and information technology systems," including by "facilitating both the intra- and inter-agency "sharing and consolidation of unclassified agency records."[122]

The DOGE EO's claimed purpose is to "maximize governmental efficiency and productivity."[123] Similarly, the Information Silo EO's claimed purpose is to remove "unnecessary barriers to Federal employees accessing Government data and promoting inter-agency data sharing" to help eliminate "bureaucratic duplication and inefficiency" and "detect overpayments and fraud."[124] But the orders' necessary effects, where agencies comply, is to strain the Privacy Act and agency-specific protections to breaking. Almost immediately after the DOGE EO went into effect, DOGE actors began seeking to gain access to, and in some cases control of, many systems, an effort fueled by the Information Silos EO. A very partial list includes: "highly restricted government records" held by the Office of Personnel Management;[125] the Treasury payments system and the deeply confidential data that makes it run;[126] Social Security Administration data, which includes

---

[121] Exec. Order No. 14343, 90 C.F.R. 42683 (Mar. 20, 2025).
[122] *Id.* § 3(a).
[123] Exec. Order No. 14158, 90 C.F.R. 8441, § 1 (Jan. 20, 2025).
[124] *Id.* § 1.
[125] Isaac Stanely-Becker, Greg Miller, Hannah Natanson & Joseph Menn, *Musk's DOGE Agents Access Sensitive Personnel Data, Alarming Security Officials*, WASH. POST (Feb. 6, 2025), https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security [https://perma.cc/F2JV-H8DN].
[126] *See* Nathan Tankus, *Elon Musk's Attempt to Control the Treasury Payments System Is Incredibly Dangerous*, ROLLING STONE (Feb. 3, 2025), https://www.rollingstone.com/politics/politics-features/trump-elon-musk-

"personal, confidential, sensitive, and private information" held on nearly every person in the United States regarding employment, retirement benefits;[127] and "the key to the IRS data vault" containing data on U.S. taxpayers.[128]

Agencies, or people there, have tried to resist. Some officials have resigned rather than carry out administration demands to circumvent protections on agency systems and data. Still, in the end, the administration appears to have made it into many sensitive systems.[129]

In every case, federal databases and data—including Americans' most deeply personal information—are being accessed, transferred, and used for purposes well beyond those for which the data was collected and outside of the legal structures that have protected that information, and kept the public's trust, for many decades. The Privacy Act is, of course, a key protection; specific laws and practices also apply at the agencies. To take just one example, taxpayer data is protected by one of the strongest privacy and confidentiality rules on the books, implemented by the IRS through meticulously strict process and technical controls.[130]

---

treasury-payment-system-dangerous-1235254831 [https://perma.cc/C7PM-S9R9].

[127] Stephen Fowler & Jenna McLaughlin, *DOGE Says It Needs to Know the Government's Most Sensitive Data, but Can't Say Why*, NPR (Mar. 26, 2025), https://www.npr.org/2025/03/26/nx-s1-5339842/doge-data-access-privacy-act-social-security-treasury-opm-lawsuit [https://perma.cc/5ZRK-FLG9].

[128] *See* Howard Gleckman, *How DOGE's Access to IRS Data Puts Taxpayer Information at Risk*, TAXVOX, Feb. 20, 2025, https://taxpolicycenter.org/taxvox/how-doges-access-irs-data-puts-taxpayer-information-risk [https://perma.cc/3UF6-84S7]; Internal Revenue Serv., *Memorandum of Understanding Between the U.S. Department of the Treasury, Internal Revenue Service, and the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, for the Exchange of Information for Nontax Criminal Enforcement*, DEP'T OF THE TREASURY (filed May 13, 2025) [hereinafter *Interdepartment Information Exchange*], https://storage.courtlistener.com/recap/gov.uscourts.dcd.278147/gov.uscourts.dcd.278147.68.1_3.pdf [https://perma.cc/A8A3-A7HL].

[129] *See, e.g.*, *Interdepartment Information Exchange*, *supra* note 128

[130] *See, e.g.*, INTERNAL REVENUE CODE, 26 U.S.C § 6103, INTERNAL REVENUE SERV., PUBL'N. 1075: TAX INFO. SEC. GUIDELINES FOR FED,

The IRS is one example, but each agency has strong protections in place—silos, if you like. In the post-Watergate era, career officials and administrations spanning the political spectrum alike have understood that Americans must trust that the government will respect and protect our most personal information, in order for taxes to be collected, Social Security benefits to accrue and be dispersed, the Census Bureau to fulfill its constitutional role—in order for the government to represent and serve the people.

Unfortunately, though the initial justification was to root out fraud and enhance efficiency, the administration very quickly began to take steps that reveal other purposes entirely. For the IRS, one purpose is explicitly to identify people for ICE to deport.[131] And now, another stated purpose has come to light: to seek out "left-leaning groups" with views disfavored by the current administration to "pursue criminal inquiries" against them under the tax laws.[132]

These extraordinary uses of federal agency power echo precisely the abuses revealed and curtailed in the Nixon era. President Nixon also attempted to politicize and weaponize the IRS, with his deputy John Dean complaining that the IRS refused to go after "foundations that feed left wing political causes," provide information "regarding our political enemies," or commence audits of "persons who [in Dean's view] should be audited."[133] In 1970, the Attorney General's

---

STATE, AND LOCAL AGENCIES: SAFEGUARDS FOR PROTECTING FEDERAL TAX RETURNS AND RETURN INFO., https://www.irs.gov/pub/irs-pdf/p1075.pdf [https://perma.cc/S2TW-VPFN].

[131] *See* William Turton, Chrisopher Bing & Avi Asher-Schapiro, *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, PROPUBLICA (July 15, 2025), https://www.propublica.org/article/trump-irs-share-tax-records-ice-dhs-deportations [https://perma.cc/N2F9-KWY8].

[132] Brian Schwartz, Richard Rubin & Joel Schectman, *Trump Team Plans IRS Overhaul to Enable Pursuit of Left-Leaning Groups*, WALL ST. J. (Oct. 15, 2025 20:00 ET), https://www.wsj.com/politics/policy/trump-irs-investigations-left-leaning-groups-democratic-donors-612a095e [https://perma.cc/7CKZ-RDUE].

[133] Joseph J. Thorndike, *Tax History: Nixon Aide Tried to Weaponize the IRS by Pressuring the Commissioner*, TAX NOTES (Mar. 13, 2023),

office sent a list of up to 12,000 "'anti-war activists and other dissidents'" to the IRS, which investigated or audited many of them, "in some cases merely because they were on the list."[134] These included both well-known names (such as Caesar Chavez, Sammy Davis, Jr., and Coretta King) and "[o]rdinary citizens," including a "local civil rights worker" and "'a bearded militant who writes and recites poetry.'"[135]

And all of these extraordinary uses of federal agency power rely on using Americans' personal information about each of us. This is a seismic rupture in the privacy-protective structures that were imposed on federal agencies in the post-Watergate era. For decades, agencies have cultivated the public trust that was lost in the wake of the Church Committee's findings by adhering to both the Privacy Act and agency-specific laws; the new administration is dismantling this protective framework. In addition to the specific harms caused by breaching information protections in this way, we now "face a crisis of public trust" at least as severe as the one the Church Committee identified.

So, collectively, we again face a truth that, in the U.S., we perhaps still haven't grappled with fully: privacy is a fundamental right. That truth is exquisitely apparent today—and more apparent, perhaps because it is under attack. At the same time, we also face the practical truth of data governance: data are unruly. They are non-rivalrous and like to leak. They

---

https://www.taxnotes.com/tax-history-project/tax-history-nixon-aide-tried-weaponize-irs-pressuring-commissioner/2023/03/10/7g45r [https://perma.cc/WSA7-Y74M].

[134] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, 80 (Apr. 26, 1976). *See also* Eileen Shanahan, *An Explanation: The Allegations Nixon's I.R.S. Interference*, N.Y. TIMES, June 14, 1974, at 12, *available at* https://www.nytimes.com/1974/06/14/archives/an-explanation-the-allegatoins-of-nixons-irs-interference-many.html [https://perma.cc/H4LW-VYTE] (describing how more than 600 names of Nixon's 'enemies' were also sent to the IRS).

[135] *Id.* at 80-81. Details contained within single quotation marks are the Attorney General's descriptions.

can only be protected by laws, by the processes and systems surrounding them, and by good-faith norms.

And this brings me back to the role of the states in privacy. Where states were building a new foundation for data privacy before this year, now, their efforts are paramount. The Information Silos EO doesn't refer only to data held by federal agencies; it also demands that Agency heads "ensure that the Federal Government has unfettered access to comprehensive data from all State programs that receive Federal funding, including, as appropriate, data generated by those programs but maintained in third-party databases."[136] States hold enormous amounts of data about their residents: voter information, records of recipients of Medicaid and food assistance programs, motor vehicle records, and more—and the federal government has wasted no time in demanding it.[137]

We face two urgent tasks that must be part of data governance: reinstating and strengthening federal protections

---

[136] Exec. Order No. 14, 343, 90 C.F.R. 42683 (Mar. 20, 2025), at § 3(c).

[137] *See, e.g.*, Jude Joffe-Block, *At Least 27 States Turn Over Sensitive Information About Food Stamp Recipients to USDA,* NPR (Oct. 16, 2025, 12:55 AM ET), https://www.npr.org/2025/10/16/nx-s1-5533045/snap-privacy-usda-lawsuit [https://perma.cc/A2JX-4UNY]; Jonthan Shorman, *Some Republican States Resist DOJ Demand for Private Voter Data*, STATELINE, (Sept. 18, 2025, 5:00 AM), https://stateline.org/2025/09/18/some-republican-states-resist-doj-demand-for-private-voter-data/ [https://perma.cc/6C9C-AQXR]; Eileen O'Connor, *Justice Department Has Demanded Voter Files from at Least 27 States*, BRENNAN CTR. FOR JUSTICE, (Sept.15, 2025), https://www.brennancenter.org/our-work/analysis-opinion/justice-department-has-demanded-voter-files-least-21-states [https://perma.cc/D7FM-FGD4]; Emily Badger, *States Have More Data About You Than the Feds Do. Trump Wants to See It*, N.Y. TIMES, Aug. 1, 2025, https://www.nytimes.com/2025/08/01/upshot/trump-states-data-privacy.html [https://perma.cc/HQ6L-TY4Z]; Jude Joffe-Block, *The Trump administration is making an unprecedented reach for data held by states*, NPR (June 24, 2025, 5:00 AM ET), https://www.npr.org/2025/06/24/nx-s1-5423604/trump-doge-data-states [https://perma.cc/66XQ-2LV5]; Emily Badger, *States Have More Data About You Than the Feds Do. Trump Wants to See It*, N.Y. TIMES (Aug. 1, 2025), https://www.nytimes.com/2025/08/01/upshot/trump-states-data-privacy.html [https://perma.cc/RYT9-7ST9].

for personal data; and building in the states, not just a "patchwork" of laws, nor even a series of experiments in the "laboratory of democracy," but a privacy *immune system*. States should buttress their privacy laws to protect their people's data and vigorously enforce those laws. And they should just as vigorously oppose any attempts by Congress to preempt their protections.

Finally, the ongoing acts by the federal government highlight the centrality of data privacy to data governance—when considering approaches to data governance, it is crucial to consider privacy, because our data privacy is vital to our ability to work, to live freely, to learn, and to participate in our own democratic governance.