PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

PRIVACY LAW SECTION JOURNAL

PRIVACY LAW

INSIDE THIS ISSUE

INTRODUCTION FROM THE PRIVACY LAW SECTION CHAIR
By Nick Ginger
PAGE 4

LETTER FROM THE EDITORS
By Jennifer L. Mitchell, Robert Tookoian and Kewa Jiang
PAGE 5

UPDATES IN PRIVACY LITIGATION: AN OVERVIEW OF ANOTHER YEAR OF EXPLOSIVE GROWTH
By Elaine F. Harwell and Yulian Kolarov
PAGE 6

SPOTLIGHT ON MICHAEL MACKO, HEAD OF ENFORCEMENT, CALIFORNIA PRIVACY PROTECTION AGENCY
By Jennifer L. Mitchell
PAGE 12

THE EVER-EVOLVING ROLE OF THE CHIEF PRIVACY OFFICER- TURNING CHALLENGE INTO OPPORTUNITY
By Kim Richardson
PAGE 18

CALIFORNIA VOTES TO ESTABLISH NEW PRIVACY LAW SPECIALIZATION
By Jeewon Kim Serrato
PAGE 22

IS CALIFORNIA LEADING THE WAY ON AI OR JUST CAUSING CHAOS?
By Susan Rohol
PAGE 26

STATE PRIVACY LAW IN 2025- WHAT TO EXPECT
By Justin Yedor and Taylor Bloom
PAGE 31

WAKE NOW, DISCOVER THAT YOU ARE A DATA BROKER
By Ben Isaacson
PAGE 33

PRIVACY LAW SECTION OFFICERS, EXECUTIVE COMMITTEE AND EDITORIAL BOARD

OFFICERS:

CHAIR

Nicholas Ginger
Carlsbad

TREASURER

Andrew Scott
Larkspur

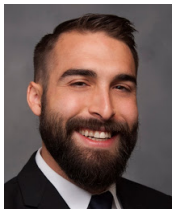
VICE CHAIR

Hailun Ying
San Mateo

IMMEDIATE PAST CHAIR

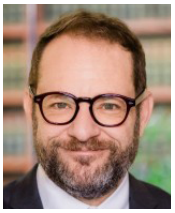
Sheri Rockwell
Los Angeles

SECRETARY



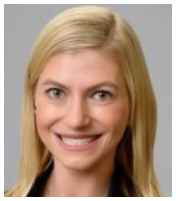
Cody Venzke
Washington D.C.

CLA BOARD REPRESENTATIVE:



Joshua de Larios-Heiman
San Francisco

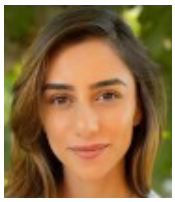
EXECUTIVE COMMITTEE:



Taylor Bloom
Costa Mesa

Jennifer L. Mitchell
Los Angeles

Brett Cook
Fort Worth, TX

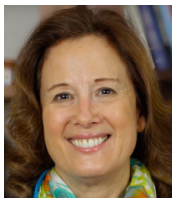


Hina Moheyuddin
Hollister

Elaine Harwell
San Diego

Jeewon Serrato
San Francisco

Paul Lanois
Paolo Alto

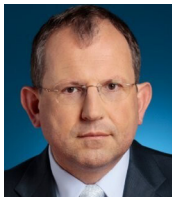


Jennifer Sheridan
San Francisco

Steven Millendorf
San Diego

Jonathan Tam
San Francisco

ADVISORS:



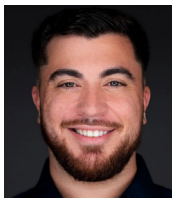
Christan Hammerl
Walnut Creek

Robert Tookoian
Fresno

LIAISON:

Gicel Tomimbang
Los Angeles

SECTION MANAGER:



Johnny Brooks
Sacramento

EDITORIAL BOARD:

Jennifer L. Mitchell
Los Angeles

Robert Tookoian
Fresno

Kewa Jiang
Oakland

WRITTEN BY

Nick Ginger

INTRODUCTION FROM THE PRIVACY LAW SECTION CHAIR

Welcome to the Second Edition of the Privacy Law Section's Annual Journal. For the second year in a row, we have put together a collection of articles offering insight, perspectives, and hopefully clarity, on issues foremost on the minds of privacy attorneys. In my introduction last year, I referenced the rapid development of the privacy landscape that had occurred since our Section's inception. Those developments have only quickened in their pace, and as we head into the beginning of a new Administration, it is anyone's guess what we can expect on the federal level over the next four years. Clearly, when it comes to privacy, there is still much to be seen.

There is also much to learn. The dizzying pace of both technological advancement and regulatory development creates a risk that society might misalign the two. It is incumbent upon us as privacy professionals to stay vigilant and ensure we mitigate that risk where we have the power to do so. We do this by availing ourselves of every opportunity to advance our understanding of technology and the law. It is imperative that we help spread this knowledge at all levels of our respective organizations and clients. It is also imperative that we participate in the law-making process. Whether this means participating in public comments for proposed legislation or advocating on behalf of privacy principles where we can, it is our duty as privacy professionals to lend our expertise to these endeavors.

By now, I hope that you can see the direction I'm headed in with this introduction. Where can an enterprising privacy professional go to help ensure they can reach their full potential? How can privacy attorneys ensure that they are on the cutting edge of developing legal issues? Where can we find like-minded professionals to deliberate the finer points of privacy law? I submit to you the answer to all these questions and more lies within becoming actively engaged with the Privacy Law Section. We are continuing to build and improve the Section, but the future of the Section relies on new volunteers stepping up to help. I encourage all those reading this to reach out and ask how you can make the Privacy Law Section reach its full potential. No matter your background, or area of expertise, there is a place for you in privacy.

Nick Ginger

Nick Ginger

Chair, Executive Committee

LETTER FROM THE EDITORS

WRITTEN BY

Jennifer L. Mitchell

Robert Tookoian

Kewa Jiang

Has it already been a year since the publication of our Inaugural Privacy Law Section Journal? It is with great pride and gratitude that we have curated another set of scholarship from some of the privacy profession's foremost thought leaders, as they delve into this year's most challenging technology and legal issues. How have privacy litigation trends evolved in 2024, and what are the newest U.S. state privacy laws to follow California's lead? We share perspectives on developments in AI, privacy litigation and privacy compliance, and California's Delete Act. Our contributors also provide valuable information about the state of our profession, from exciting updates on the legal specialization in Privacy Law, to unique perspectives on the role of the Privacy Officer straight from an in-house privacy lawyer. Last but certainly not least, we are pleased to present special insights from an interview with Michael Macko, Head of Enforcement at the California Privacy Protection Agency (CPPA).

Established in 2020, the Privacy Law Section is the newest section within the California Lawyers Association, and we have come a long way. The mission of the Privacy Law Section is to bring together privacy practitioners working in diverse settings, to provide members with a range of unique educational opportunities, and to allow for an exchange of ideas and technical expertise. Our members include privacy attorneys working in practice settings ranging from private practice to in-house privacy and cybersecurity roles, as well as consumer privacy advocates, government regulators, and policy analysts at privacy think tanks.

We again invite you to join our dynamic and accomplished group of privacy leaders in the Section's year ahead, as we would not be here without your active contributions. We also hope to see you back in Los Angeles at our Third Annual Privacy Summit from February 27-28, 2025.

We would like to thank all of our contributors for volunteering their time, enthusiasm and expertise. As always, we are appreciative that each of you chose to be a member of our community.

Jennifer L. Mitchell
Executive Committee Member
Chair of Privacy Publications

Robert Tookoian
Advisor
Vice-Chair of Privacy Publications

Kewa Jiang
Vice-Chair of Privacy Publications

WRITTEN BY*

Elaine F. Harwell

Yulian Kolarov

UPDATES IN PRIVACY LITIGATION: AN OVERVIEW OF ANOTHER YEAR OF EXPLOSIVE GROWTH

Over the last couple of years, as privacy has become increasingly important to consumers, courts and companies have seen a significant increase in privacy litigation. In this article, we will look at some of the notable data privacy-related litigation trends of the last year, including under California state law claims based on the California Invasion of Privacy Act ("CIPA") and the Investigative Consumer Reporting Agency Act ("ICRAA"), federal statutory claims, including the Video Privacy Protection Act ("VPPA"), and recent rulings in data breach litigation.

CALIFORNIA INVASION OF PRIVACY ACT

As many privacy practitioners are aware, plaintiffs–who are visiting websites, filling out forms on websites, entering search terms on websites, or chatting with chatbots–are pursuing litigation against website owners claiming their interactions with the websites are "communications" and the sharing of their data to third parties without their consent violates their privacy rights. In making the claims, plaintiffs have resurrected multiple statutes, including CIPA, a decades-old statute originally enacted to prevent eavesdropping on telephone calls. The new CIPA cases, however, focus on extending the statute to the alleged unlawful use of website tracking technologies, such as pixels and cookies, that collect, use, and share personal information of website visitors with third parties. Thus far, courts encountering these cases have been inconsistent with their holdings, and very few cases have reached summary judgment.

Many of the lawsuits and arbitration demands have centered around a few key arguments:

WIRETAPPING CLAIMS

While CIPA is a bigger statute, the focus for these cases has been in the context of wiretapping claims. Plaintiffs generally bring claims under California Penal Code section 631(a), which prohibits four types of activities:

1. Intentional wiretapping;
2. Willfully attempting to learn the contents or meaning of a communication in transit over a wire;
3. Attempting to use or communicate information obtained as a result of wiretapping or obtaining the contents of a communication; and
4. Aiding, agreeing with, employing, or conspiring with another party to engage in the prohibited activities above.

Plaintiffs have also brought actions under California Penal Code section 632 for eavesdropping or recording of a confidential communication without consent. If found liable, companies may be at risk of paying $5,000 per violation. Expectedly, class actions have been common.

Although litigation has progressed over the last couple of years, there does not appear to be much rhyme or rhythm to how courts are handling motions to dismiss at the pleading stage. In the recent case of *Doe v. Google LLC*,[1] the plaintiffs sued Google for its source code located on health care providers' websites. The court granted Google's motion to dismiss the CIPA claim because the complaint failed to allege "where on a web property [Google's] source code actually exists."[2] The court also held that Google did not "intentionally" collect confidential information because it warned and prohibited the companies that use the Google source code not to send Google any personal health information.[3]

Interestingly, there is some disagreement in the federal courts as to whether Google and Meta's policies are sufficient to resolve the intent prong at the motion to dismiss stage. The court in *Doe v. Google LLC* noted that it is "possible that this ruling is contrary to Judge Orrick's analysis of intent in a similar pixel case against Meta,"[4] where Judge Orrick in a different district court case determined that the complaint sufficiently alleged Meta routinely ignored its own policy.[5] To contrast, in another 2024 Meta Pixel case, the court held along the same lines as Judge Orrick and determined Meta's policy prohibiting customers from transmitting data was a question of fact that could not be resolved at the motion to dismiss stage.[6]

In June 2024, the Northern District of California denied Google's motion to dismiss a class action complaint alleging that Google Analytics, deployed on various tax websites, collected their gross income and refund amounts without their consent in violation of CIPA.[7] Ultimately, the court disagreed that Google was a "mere vendor" of the tool because Google read the data collected by its tool and benefited and profited from it by creating a "detailed dossier, or digital fingerprint" for each user.[8] Despite Google's policy that explicitly prohibits its customers and developers from sending personally identifiable data, the court determined that it could not resolve this question of fact at the motion to dismiss stage. This is again contrary to the court in *Doe v. Google LLC*, which found a similar Google policy to be more convincing in finding lack of intent.

Notably, at least one California district court has ruled on a motion for summary judgment in the context of CIPA. In *Gutierrez v. Converse*, the defendant's website contained a chat feature run by a third-party vendor.[9] Messages sent through the chat were transmitted from the consumer's device to the defendant's cloud application on the third-party server.[10] The chats, however, were fully encrypted while in transit, and the third party did not have access to the server unless a defendant granted access.[11] Plaintiff, in a putative class action, claimed that she did not consent to the sharing of her communications with the third party when she accessed the chat through her mobile device.[12] The district court granted summary judgment for the defendant, finding:

1. The third-party did not intentionally wiretap because plaintiff presented no evidence from which a reasonable jury could conclude the website involved telephone communications. Instead, the evidence indicated plaintiff used her smart phone's internet capabilities by accessing the website on her phone.
2. The third-party did not willfully attempt to learn the contents of a communication while in transit because the evidence showed all messages sent through the chat were encrypted. Furthermore, the third-party vendor could not access any data stored on its servers.
3. Because plaintiff failed to show there was an intentional wiretap or an attempt to learn the contents of a communication in transit, defendant could not be liable for aiding and abetting.[13]

As of this writing, the case pending on appeal before the Ninth Circuit, which may finally rule on these issues.

PEN REGISTER CLAIMS

There has also been a recent rise in claims under California Penal Code section 638.51, which prohibits the use of "pen registers" and trap and trace devices to record or capture "dialing, routing, addressing, or signaling information" from a "wire or electronic communication." In two similar cases, *Anne Heiting v. Taylor Fresh Foods, Inc.* (California Superior Court),[14] and *Dino Moody v. C2 Educational Systems Inc. et al.* (United States District Court for the Central District of California),[15] the plaintiffs claimed that TikTok software deployed on defendants' websites consisted of a "pen register" or "trap and trace" device under the statute.

At issue in both cases was TikTok's software that allegedly uses "fingerprinting," a process where the website employing

the software collects data from anonymous visitors and matches that data with TikTok's database to uncover the visitors' identities. This is achieved by accessing a website user's device and browser information, geographic information, referral tracking, and URL tracking. The software is designed to capture phone numbers, emails, routing, addressing and other signaling information of website visitors, and it does so in some instances without the website visitors' consent.

The defendant in each case challenged the complaint for failure to state a claim. In *Moody*, defendant contended section 638.51 was intended to regulate *physical* trap and trace devices such as those attached to telephone lines—not website software.[16] Defendant further argued that the TikTok software had been consented to and that it did not collect dialing routing, addressing, or signaling information in violation of the statute.[17] The court denied defendant's motion to dismiss finding that CIPA was not limited to physical devices, and that the inclusion of "electronic communication" in the language of the statute sufficiently covered software.[18] The court also did not find persuasive that defendant was the "user" of the software and therefore consented by installing TikTok software on its website. For at the least the motion to dismiss stage, the court found it a possibility that the plaintiff was the relevant user under the statute.[19]

The *Anne Heiting* court went further and stated that upholding Defendant's definition of the consent exception would lead to the absurd result that section 638.51 could never be violated, and it would be inapposite to CIPA's express purpose of protecting California residents' right to privacy.[20]

Whether these claims ultimately succeed is yet to be determined, but it is notable that the courts are at least willing to entertain the allegations.

VIDEO PRIVACY PROTECTION ACT

Another privacy statute that entered 2024 with a strong showing in courts was the VPPA, which makes it unlawful for a "video tape service provider" to "knowingly disclose[], to any person, personally identifiable information concerning any consumer of such provider."[21] The statute further defines "consumer" as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[22] This 1988 statute was revived by plaintiffs in recent years to fit newer technology under its umbrella.

In an interesting twist to VPPA litigation in the Northern District of Ohio, plaintiffs, in the case *Collins v. The Toledo Blade*, alleged they subscribed to newspaper websites and received usernames and passwords.[23] In return, the newspapers allowed plaintiffs access to their websites where they could watch pre-recorded and live-stream videos.[24] Using the Meta Pixel, plaintiffs alleged the websites tracked when plaintiffs accessed a video on the websites and subsequently sent identifying information about the web visitor, including Facebook IDs, and video-watching information to Meta.[25] Defendants filed a motion to dismiss and ultimately the *Collins* court denied the motion finding that disclosure to a third party alone constitutes an injury under the statute.[26] It also held that plaintiffs' complaint plausibly alleged they were "subscribers" because they signed up to receive more than a periodic newsletter or email–they also signed up to receive access to the website.[27]

In another recent VPPA case, *Salazar v. NBA*, the Second Circuit breathed additional new life into the statute by expanding the definition of a "subscriber."[28] In *Salazar*, plaintiff signed up for a free online NBA newsletter and later watched videos on the NBA's website.[29] Plaintiff further alleged each time he viewed a video, the NBA disclosed his Facebook ID and video-watching history to Meta without his permission through an embedded pixel.[30] Plaintiff asserted this behavior violated the VPPA. Initially, the district court dismissed the case on the reasoning that the VPPA only applied to "subscribers" and the act of signing up for an online newsletter did not make plaintiff a "subscriber" of goods or services from a "video tape service provider."

The Second Circuit, however, reversed and held that a subscriber of *any* goods or services is a "subscriber" under the VPPA. In short, the court expanded the definition of consumer by not limiting standing under the VPPA to those individuals that paid to consume video or audio content from a business for purposes of the statute.[31] The Second Circuit's simple yet impactful holding may provide guidance for lower courts that have produced conflicting opinions on what type of interactions would make a plaintiff a "subscriber" under the VPPA.

Although it appears the Ninth Circuit has yet to specifically address the issue of what defines a consumer under the VPPA, businesses should be cognizant that asking consumers to subscribe to *any* goods or services, even a free online newsletter, might make them subject to the VPPA and potential violations.

INVESTIGATIVE CONSUMER REPORTING AGENCY ACT

In another novel use of a decades-old California statute, numerous lawsuits have recently been filed asserting violations of the California Investigative Consumer Reporting Agency Act ("ICRAA").[32] ICRAA places specific obligations on investigative consumer reporting agencies– and anyone who uses investigative consumer reports– with regard to the procurement of background reports, including those typically used by employers and landlords for employment and rental decisions. Anyone requesting an "investigative consumer report" must notify the consumer "not later than three days after the date on which the report was first requested," including the name and address of the investigative consumer reporting agency.[33] A consumer must also be provided with "a means by which the consumer may indicate on a written form, by means of a box to check, that the consumer wishes to receive a copy of any report that is prepared," including the name of the reporting agency.[34] Failure to do so may result in liability for actual damages sustained or $10,000, whichever is greater, per violation.[35] The statute also allows for punitive damages for conduct that is grossly negligent or willful.[36]

Recently, numerous lawsuits have been filed against property managers claiming rental applications did not comply with ICRAA's disclosure requirements or copies of reports were not provided pursuant to the law. Case law is minimal in this area, but notably, there are at least two California superior courts that have come down on different sides as to whether plaintiffs, who arguably suffered no damage, have standing to bring ICRAA claims. In *Busane v. WSH Management, Inc.*,[37] the court answered in the affirmative. In a relatively short order, the court dismissed the defendant's contentions that the plaintiffs lacked standing because their rental applications were accepted, and as such, no adverse action was taken against them.[38] The court, however, only found it relevant that the reports were requested, which triggered ICRAA obligations with which the defendant allegedly did not comply.[39] The court interpreted the statutory allowance of $10,000 per violation as a penalty, regardless of whether plaintiffs showed harm, and thus the plaintiffs were found to have standing.

In a separate California superior court case, *Yeh. v. Barrington Pacific, LLC*, the court found the plaintiffs, who successfully rented apartments, lacked standing because they were not harmed.[40] In a far lengthier opinion, the court relied on a California Court of Appeals' opinion in *Limon v. Circle K Stores Inc.*, which involved similar arguments under the Fair Credit Reporting Act ("FCRA").[41] The court analogized ICRAA to the FCRA, which contained a similar provision for damages, and agreed with the *Limon* court's legal and linguistic analysis of "damages" and "penalties".[42] In reviewing the intent of the California Legislature in passing ICRAA, the court determined that the use of the terms "penalty" and "damages" in the same discussion indicated a lack of clear intent to distinguish between damages sustained and the $10,000 cap on recovery.[43] Ultimately, the court held that because the statute provided for damages, not penalties, plaintiffs were required to show they suffer an actual and concrete injury.[44] Because plaintiffs' rental applications were ultimately approved, and none of the information disclosed in the reports was inaccurate, they did not suffered an injury and therefore lacked standing.[45] As of this writing, the trial court order dismissing the coordinated *Yeh* cases is up on appeal.

DATA BREACH LITIGATION

For most companies, one of the main risks following a data breach is facing a potential class action lawsuit. Plaintiffs generally assert various claims, including contract and negligence claims, and various duties to protect personal information under federal and state statutes with a private right of action. A full overview of current data breach litigation is beyond the scope of this article. However, a couple of recent decisions are worth noting.

In one unpublished decision by the Ninth Circuit, the court focused on the language of a data breach notification letter in upholding a lower court dismissal of a plaintiff's complaint for lack for standing.[46] There, the plaintiffs asserted a common argument that they had Article III standing because of an increased future risk of identity theft from a cyberattack, which had compromised driver's license numbers.[47] Plaintiffs relied on a notice that defendant Noblr Reciprocal Exchange ("Noblr") had sent to more than 90,000 individuals several months after the attack.[48] The notice stated that the cyber attackers "may" have had access to driver's license numbers and addresses.[49]

The Ninth Circuit found plaintiffs did not have standing because Noblr's notice did not explicitly state whether any of the plaintiffs' driver's license numbers were actually stolen, only that those numbers may have been exposed.[50] That alone, according to the court, was insufficient to show injury. Although unpublished, the opinion highlights the importance of the language used in data breach notices sent to impacted individuals.

Additionally, companies that have suffered a data breach must also consider what information from a post-breach investigation may end up being subject to discovery. Where a company–or its outside counsel–hires a computer forensics examiner to investigate an incident, a report on the cause and scope of the incident often follows. Some companies have successfully shielded the forensic reports from disclosure in subsequent litigation under the work product doctrine or attorney-client privilege. Several recent court opinions, however, have rejected these claims of privilege, including a recent New Jersey district court held that certain documents shared between Samsung, its outside counsel, and a retained cybersecurity consulting firm, Stroz, were not protected and subject to disclosure.[51] At issue were documents consisting of PowerPoint updates on investigative findings, an analysis outlining conclusions regarding the background and scope of the incident, and a document prepared by the consulting firm to be shared with the FBI.[52]

Following an *in camera* review, the district court scrutinized whether the documents were intrinsic to the attorney client communication and an understanding of legal advice being rendered to Samsung, as opposed to some other business purpose.[53] The court determined that the above documents were not covered by attorney-client privilege based on the following findings:

- The PowerPoint documents and meetings were merely investigative findings that detailed how the breach had occurred. Present at the meetings were multiple IT and high-level executives outside of the legal department. The executives were "receiving" information from Stroz rather than providing or facilitating information gathering for the purpose of obtaining legal advice.
- The reports outlining conclusions were shared with fifteen different high-level executives, including Samsung's security response team. The breadth of Samsung's involvement and participation in Stroz's investigative process, in addition to the wide dissemination of the documents, indicated Stroz was retained only to provide technical interpretation.
- The FBI report was found to have been drafted for business reasons, including to respond to inquiries from the FBI. There was no showing that the report was related to a litigation purpose.[54]

Moreover, the mere fact that it was Samsung's outside counsel that hired Stroz to perform a business function was not enough to shield the documents from production based on attorney client or attorney work-product privilege.[55]

Ultimately, for post-breach forensic reports, the court will employ a fact-intensive analysis to assess privilege claims. Companies must be able to demonstrate the primary purpose of the forensic report was to seek legal advice. Additionally, outside counsel's retention of cybersecurity consultants will not automatically cloak all communications under a blanket of privilege. In order to maximize the ability to successfully assert privilege over a post-breach report, it is important to follow best practices outlined by recent case law.

CONCLUSION

Data privacy litigation has seen a surge in recent years, a trend which is likely to continue as companies continue to collect, use, and share more data. Meanwhile, the plaintiffs' bar is continuing to find creative uses of decades-old statutes to assert various privacy violations. As the courts continue to grapple with these issues, businesses would be wise to visit how their data policies and procedures align with emerging guidance.

ENDNOTES

* Elaine F. Harwell is a Partner at the law firm of Procopio, Cory, Hargreaves & Savitch, LLP. Elaine focuses on representing clients in privacy and data security matters, including litigating claims involving privacy issues, helping clients manage emerging risks, and advising on regulatory and compliance issues. Elaine has earned the ANSI-accredited Certified Information Privacy Professional/United States (CIPP/US) and the Certified Information Privacy Manager (CIPM) credentials through the IAPP and is the leader of Procopio's Privacy and Cybersecurity practice and the firm's Privacy Officer.

Yulian Kolarov is an Associate at the law firm of Procopio, Cory, Hargreaves & Savitch, LLP. Yulian assists clients with a wide range of business disputes and civil litigation, including matters involving privacy, cybersecurity, contracts, real property, corporate governance, and partnership and business management disputes. He previously clerked with the Honorable Daniel E. Butcher of the U.S. District Court for the Southern District of California.

1. Doe I v. Google LLC, No. 23-CV-02431-VC, 2024 WL 3490744 (N.D. Cal. July 22, 2024).
2. Id. at *6.
3. Id.
4. Id. at *5.

5. Doe v. Meta Platforms, Inc., 690 F. Supp. 3d 1064, 1076 (N.D. Cal. 2023).
6. In re Meta Pixel Tax Filing Cases, No. 22-CV-07557-PCP, 2024 WL 1251350, at *4 (N.D. Cal. Mar. 25, 2024).
7. Smith v. Google, LLC, No. 23-CV-03527-PCP, 2024 WL 2808270 (N.D. Cal. June 3, 2024).
8. Id. at *5.
9. Gutierrez v. Converse Inc., No. CV 23-6547-KK-MARX, 2024 WL 3511648, at *2 (C.D. Cal. July 12, 2024).
10. Id.
11. Id. at *3.
12. Id. at *1.
13. Id. at *7–8.
14. Anne Heiting v. Taylor Fresh Foods, Inc., Superior Court of California, County of Los Angeles, 24STCV12891 (July 31, 2024) (Minute Order Denying Demurrer).
15. Moody v. C2 Educ. Sys. Inc., No. 2:24-CV-04249-RGK-SK, 2024 WL 3561367, at *2 (C.D. Cal. July 25, 2024).
16. Id. at *2.
17. Id.
18. Id. at *2–3.
19. Id. at *3.
20. Anne Heiting v. Taylor Fresh Foods, Inc., Superior Court of California, County of Los Angeles, 24STCV12891 (July 31, 2024) (Minute Order Denying Demurrer).
21. 18 U.S.C. § 2710(b)(1).
22. Id. at (a)(1)
23. Collins v. Toledo Blade, 720 F. Supp. 3d 543, 546 (N.D. Ohio 2024).
24. Id.
25. Id.
26. Id. at 549–51
27. Id. at 551–53.
28. Salazar v. Nat'l Basketball Ass'n, 118 F.4th 533 (2d Cir. 2024)
29. Salazar v. Nat'l Basketball Ass'n, 118 F.4th 533 (2d Cir. 2024)
30. Id. at 537–38.
31. Id. at 550–53.
32. Cal. Civ. Code § 1786.
33. Id. at § 1786.16(a)(3)
34. Id. at § 1786.16(b)(1).
35. Id. at § 1786.50(a)(1).
36. Id.
37. Los Angeles County Superior, Case No. 22STCV29627 (Aug. 29, 2023) (Orde Granting Plaintiff's Motion for Summary Judgment).
38. Id.
39. Id.
40. Yeh. v. Barrington Pacific, LLC, Los Angeles County Superior Court, Case No. 20STCV42994 (Jan. 18, 2024) (Order Granting Defendant's Motion for Summary Judgment).
41. Id.
42. Id.
43. Id.
44. Id.
45. Id.
46. Greenstein v. Noblr Reciprocal Exch., No. 22-17023, 2024 WL 3886977 (9th Cir. Aug. 21, 2024).
47. Id. at *1.
48. Id.
49. Id.
50. Id. at *2–3.
51. In re Samsung Customer Data Sec. Breach Litig., No. CV 23-3055(CPO)(EAP), 2024 WL 3861330 (D.N.J. Aug. 19, 2024).
52. Id. at *2–3.
53. Id. at *4.
54. Id. *11–15.
55. Id. at *15.

WRITTEN BY*

Jennifer L. Mitchell

SPOTLIGHT ON MICHAEL MACKO, HEAD OF ENFORCEMENT, CALIFORNIA PRIVACY PROTECTION AGENCY

Michael Macko

Politico described Michael Macko, head of enforcement at the California Privacy Protection Agency (CPPA), as "one of the most powerful privacy enforcers in the U.S."[1] It's easy to see why. Between launching investigative sweeps into the practices of the connected vehicle and data broker industries, managing open privacy investigations in the "double digits and growing," bringing multiple enforcement actions, and publishing Enforcement Advisories, the CPPA's Enforcement Division has been busy. The CPPA is building its reputation as one of the most formidable privacy regulators in the nation, or perhaps the world.

I had a chance to catch up with Mike to discuss his illustrious career path, the Division's priorities, and the future of privacy. Mike came to the CPPA with nearly two decades of litigation and investigative experience, including as in-house counsel handling government and regulatory litigation in the tech industry, and as Assistant U.S. Attorney and Trial Attorney at the U.S. Department of Justice and U.S. Securities and Exchange Commission. A former adjunct professor of law, he started his career as a litigator at a large law firm and clerked for judges on the U.S. Court of Appeals and U.S. District Court.

MITCHELL: Could you please share more about your career background prior to joining the CPPA?

MACKO: Of course, and it's a pleasure to talk with you. I've spent most of my career leading government investigations. I started out as a litigator at a large law firm, and then I spent a decade prosecuting cases and handling civil litigation for the U.S. Department of Justice, mostly as an Assistant U.S. Attorney. The False Claims Act was my specialty, but I also brought cases under the Controlled Substances Act, the civil rights laws, and various white-collar fraud and healthcare fraud laws. Anything involving federal money, misuse of funds, or federal regulation.

I moved to the Securities and Exchange Commission's Enforcement Division as a Trial Attorney. I used the same types of tools to pursue violations of the securities laws, mostly insider trading cases, breach of fiduciary duty, and corporate disclosure

violations. It was fun to use my investigative techniques in a new way and in such a sophisticated industry.

I left government to join Amazon.com, Inc., as in-house counsel handling government litigation and investigations worldwide. Let's face it, all tech companies face regulatory scrutiny. It comes with the territory when you're innovating. I enjoyed helping folks navigate those issues and learned a lot advising businesses. I managed a wide variety of matters at Amazon involving consumer protection, advertising, tax, content moderation, cloud computing, and financial regulation. And, of course, aspects of data privacy.

I've been lucky to learn from talented colleagues each step of the way. Now I'm back on the government side again. I have to admit, it's been helpful to sit on both sides of the fence.

MITCHELL: How did you make the decision to pivot to privacy?

MACKO: It wasn't a pivot so much as an opportunity to build something again. At the U.S. Attorney's Office in Philadelphia, I was part of an enforcement Strike Force where I created novel theories and built pipelines of enforcement actions. I focused on financial fraud, but we pursued all sorts of investigations. It was rewarding to use our usual tools as prosecutors to build something new and different.

The CPPA was a chance to do something similar. As you know, California did something remarkable with its privacy law. It passed the cutting-edge California Consumer Privacy Act in 2018. And then California strengthened the law in 2020 through a voter initiative that created the CPPA, the only dedicated data protection authority in the United States. That was Proposition 24. The voters wanted stronger protections over their privacy, and it's our job to make that happen.

I could see the challenge of building an Enforcement Division from scratch. And I could see how we could do it. I like building teams, running complex investigations, getting results. I knew I'd get to work with Ashkan Soltani, one of the world's leading experts in tracking technology. So, that's why I made the decision. I couldn't be happier about it.

MITCHELL: Can you explain the origin of the CPPA Enforcement Division and the Division's goals?

MACKO: The original CCPA vested enforcement authority solely with the California Attorney General, similar to other state laws. But as part of Prop 24's strengthening of the law, the voters created the CPPA as a new agency and gave it enforcement authority with the Attorney General, so both can enforce the law but in different ways. The Attorney General brings the actions directly in court, while our Enforcement Division brings the actions before administrative law judges with judicial review later. The remedies are powerful regardless of the forum. Our enforcement authority became effective in July 2023. I joined as head of the Enforcement Division around the same time.

I'm so proud of the team we've built over the past year. We have the former chief privacy officer and in-house privacy counsel for major tech companies, attorneys from some of the world's largest and best law firms, and government litigators with decades of trial experience. And that's just the attorneys. We have support staff with years of experience in Legal Aid and elsewhere, and a worldclass technologist team.

Our mandate is to enforce the law vigorously. We've publicly announced several initiatives, including our ongoing investigations into connected vehicles and data broker registration. But most of our work relates to other things and takes place behind the scenes. The number of our open investigations is easily in the double digits and growing.

MITCHELL: How has your background as an in-house lawyer and at the SEC influenced your views and your vision for the CPPA Enforcement Division?

MACKO: I stepped out of a world of U.S. law enforcement—fraud cases, securities cases, consumer protection cases, you name it—and into a world of privacy law that grew out of Europe. Many businesses have evaluated their risk with a European framework in mind, or it's at least influenced them. Often this means looking at consumer privacy from the perspective of an individual consumer. Individual rights are at stake. Fundamental rights.

In many ways that's true here too, but when I've brought cases as a federal prosecutor, I've asked myself how I can benefit the largest number of people. Which cases can I bring to make the biggest impact? California law provides a monetary fine on a "per violation" basis, just like the federal False Claims Act and other laws I've enforced, so I'm looking at the totals. I'm looking at the aggregate.

Privacy professionals understand how quickly the exposure can add up, but the industry in the U.S., at the C-suite level, doesn't always make the same risk calculation. If they did, in-house privacy professionals would see more resources at their disposal. We'd see cleaner, better, and more innovative implementation of privacy protections on the tech side. Those things take resources. They require investment. I brought some of my strongest cases against businesses that made the wrong calculation, they got the allocation wrong and paid a price for it.

I know it's hard to quantify regulatory risk. But my job is to move the needle toward incentivizing businesses to invest more in compliance. I'd like to level the playing field for the businesses that *did* invest in honoring consumers' privacy rights. That means that privacy scofflaws should pay the price for their violations, and we need to make enforcement more likely. That's how we change the calculus.

MITCHELL: How does the role of the Enforcement Division differ from the role of the CPPA Audit team?

MACKO: Securities lawyers might see a parallel here with the SEC, which has a Division of Enforcement and a Division of Examinations. Some examinations result in enforcement, but the majority result in examination findings and corrective action short of enforcement.

The difference boils down to the purpose. The Enforcement Division investigates potential violations, while the Audits Division evaluates compliance. When the Enforcement Division identifies violations, we bring enforcement actions. The Audits Division makes findings that might or might not result in a referral to the Enforcement Division, just like at the SEC. It depends on the circumstances.

MITCHELL: How does it differ from the role of the CA AG's office when it comes to CPPA enforcement?

MACKO: I wouldn't want to speak for the California AG's office or draw distinctions, but the AG's office has a strong and committed team. They're real trailblazers, and we share their passion for enforcing the law. I credit Stacey Schesser from the AG's office for inspiring me to follow her path out here. Stacey and I met back in Philadelphia when we both clerked together in the Third Circuit, and we've been friends for years. Suffice it to say that we work well together in our enforcement roles, and we're very much a unified front.

MITCHELL: How do potential violations come to the attention of your team?

MACKO: For years as a prosecutor, some of my best evidence came from the inside. I relied on whistleblowers to tell me about violations. I still receive information from whistleblowers, but consumers are telling us the most. Shortly after we received our enforcement authority, we set up an online complaint system where anyone can tell us about violations, even anonymously.

Consumers heard our call and have been responding to it. Since launching the system, we've received thousands of complaints. We use those complaints to identify trends, specific violations, and evidence. It's a great resource for our team, and we review every single complaint.

But we also hear about violations from media articles, other regulators, and our own experiences engaging with businesses as consumers. On top of that, our technologists are conducting proactive research and we rely on their insights.

MITCHELL: Could you tell us about the process for investigating potential violations of the CCPA?

MACKO: I'm happy to tell you about the business-facing part. It starts with communication from us, often informal. We might share a consumer complaint and ask a business to respond. Or we might send a letter asking a business for documents or information. Sometimes we seek this information in a subpoena. If you're hearing from us, we had a reason, and I wouldn't focus too much on the form of our communication.

From there, our process is thorough. We try to determine as efficiently as possible whether a violation has occurred. We frequently meet with businesses, review multiple rounds of documents and interrogatory answers, take any necessary testimony, and take stock of what the evidence shows.

Our investigative playbook is like the one I used at the DOJ and SEC but, candidly, I'm always learning new things from state Attorneys General and our federal partners. We try to borrow the best practices of other agencies.

MITCHELL: How do you expect businesses to engage with the CPPA in an investigation?

MACKO: Direct answers are a start, even when the answers are uncomfortable. This means admitting unhelpful facts when it's appropriate. I know how hard it can be to do that, but it builds credibility. You have to remember that we've already consulted our research technologists by the time you hear from us, and we're often able to establish certain facts early on. I also expect to see timely responses to our team's communications and timely, full productions of documents.

MITCHELL: Is it the Agency's practice to issue closure letters, as is the practice with other agencies? Why or why not?

MACKO: It's rare for investigative agencies to send closure letters, and for good reason: investigations are organic. You might close an investigation one day, receive new evidence the next, and open it back up again. Or you might change your priorities or find yourself with unexpected time, and you turn back to a "closed" matter.

It works the same way for us. Sending a closure letter wouldn't give a business reassurance or actual closure given the ongoing and evolving nature of our investigations. So, it's not our practice.

MITCHELL: What are the Enforcement Division's top priorities now and what do you forecast for 2025?

MACKO: Our team has been prioritizing investigations involving privacy notices, the right to delete, and the implementation of consumer requests. By that, I mean we've been looking under the hood to see whether businesses are doing what they say when it comes to privacy rights.

For 2025, we'll be continuing those investigations but with additional nuance. For example, we'll be looking closely at businesses that honor consumer opt-out requests only if consumers verify their identity. The law is clear on that point. Businesses aren't allowed to require consumers to verify their identity to make a request to opt-out of the sale or sharing of their personal information, or to limit the use and disclosure of their sensitive personal information. The law says that businesses can ask for information necessary to complete the request, yes. But they can't go beyond that. We addressed this issue in our first Enforcement Advisory.

We'll also be looking at businesses that use dark patterns, often called deceptive design, to prevent consumers from asserting their rights. Let me pause there because this is important. "Dark pattern" isn't some nebulous buzzword. California law defines the term and gives concrete examples. Our second Enforcement Advisory dealt with an application of dark patterns.

MITCHELL: Are there particular industries or populations that the Enforcement Division is focused on?

MACKO: You're right to ask about certain populations because we're working to identify the communities most vulnerable to violations. Some of them are obvious. We know, for example, that kids don't always understand the technology or what's being asked of them. The same can be said of older citizens.

This is something close to my heart. I spent years serving on the Elder Justice Task Force for the U.S. Department of Justice, and I brought some of the most significant healthcare fraud cases that targeted older Americans in nursing homes. We're absolutely going to consider who's most vulnerable.

And it's not just age. Data brokers are categorizing groups of people in increasingly creepy ways. Are you a gun owner? A church member? A gender or sexual minority? A patient at a reproductive health clinic? You can be sure that data brokers are categorizing these groups and plenty more.

Geolocation data makes the effects even scarier. Don't take my word for it, take a look at the FTC's recent complaint against Kochava. Changes in technology can make certain groups vulnerable overnight, even if they weren't vulnerable the day before. We've got to stay ahead of it.

MITCHELL: You mentioned data brokers, and you recently announced an investigative sweep into whether data brokers are registered with the Agency. Can you share any details about that effort?

MACKO: Data brokers operate in a multi-billion-dollar industry. The participants aren't always careful about who they sell to. They don't always have the best security practices. Even small shops can have an outsize impact in harming consumers. We know this from recent data breaches like National Public Data's, which reportedly consisted of billions of records from 170 million Americans.

California law requires data brokers to register with the agency and pay an annual fee. The point of registration is to give consumers visibility, give them transparency to an industry that can operate in the shadows.

In October, we announced a crackdown on data brokers who failed to register. The next month, we announced that we'd reached settlements with two data brokers. Our board voted unanimously to approve those settlements. Additional investigations are ongoing, so you can expect to see more enforcement action here.

Data brokers are just one slice of our investigative efforts. We're working on dozens of investigations under the CCPA unrelated to data brokers. These investigations are more complex and can take longer, but we're pursuing them with the same intensity.

MITCHELL: How are Enforcement Advisories intended to be used by the Agency and how should they be viewed by businesses?

MACKO: When I handled healthcare fraud cases, I'd sometimes see agencies issue special fraud alerts to caution the industry about certain conduct. I saw similar risk alerts when I litigated securities fraud cases. These alerts told the industry something about what regulators were seeing, what they were concerned about. These alerts inspired me.

I wanted us to issue Enforcement Advisories because part of our agency's mission is to educate the public, and I'd like to maximize compliance any way I can. Advisories are a middle ground, a way for the Enforcement Division to speak

without charging a business with violations. In that sense, the advisories are purely an enforcement voice. The CPPA's board might hold a different view, and our board serves as the ultimate decision-maker in the cases we prosecute.

You'll probably see the advisories give you a preview of future enforcement actions. When we show up with an investigative request touching upon the same issues in an advisory, you can't say we didn't warn you.

MITCHELL: Do the Enforcement Advisories signal a move away from enforcement actions?

MACKO: It's the opposite. When we've issued an advisory and we still see violations, there's really no excuse. Stronger medicine will be in order.

MITCHELL: Can you tell us about the Enforcement Division's view on cross-state coordination?

MACKO: We're committed to consistency and harmony, and that's why we spend so much time coordinating with our partners in other states. In fact, you're not going to find an example where California enforced its privacy law in a way that created an inconsistency with another state. It hasn't happened.

This collaboration is baked into the CCPA. The law tells us to cooperate with other states to ensure consistent application of privacy protections, and we take that mandate seriously. Earlier this year we launched the Consortium of Privacy Regulators, a network of states that have their own comprehensive privacy laws, and I'm on the phone every week, sometimes every day, with my colleagues in other states to keep ourselves on the same page.

MITCHELL: Why has the Agency chosen to partner with the CNIL?

MACKO: We've partnered with multiple state, federal, and international data protection authorities, including the CNIL in France. We're living in a global economy, and privacy rights are a commercial reality. It's important to see international collaboration, not just the state-wide collaboration that's central to our mandate. That's why we're also members of the Asia Pacific Privacy Authorities, the Global Privacy Enforcement Network, and the Global Privacy Assembly, to name a few. You can expect to see more international collaboration in the coming year.

MITCHELL: What is your view on the future of privacy in the U.S.?

MACKO: Privacy is an issue that crosses party lines. I see states continuing to collaborate and work closely together to harmonize our enforcement approaches and promote consistency. You're already seeing state privacy laws share many of the same fundamental concepts, and I expect enforcement to reflect the same consistency. We're lucky that states can experiment like this and respond to changing technologies in such nimble ways. For example, California and Colorado have recently adopted new privacy protections for neural data. We've seen the states bolster existing protections with thoughtful ideas. No doubt that will continue.

I predict we're going to continue seeing states value their citizens' privacy. We're going to see ongoing interest at the federal level, too. Over time, we're going to see businesses take privacy violations even more seriously. When I used to show up at the door as a federal prosecutor or as an SEC attorney, businesses knew that liability could be an existential threat. We need businesses to have that reaction to privacy violations too, and vigorous enforcement is the only way to do it.

MITCHELL: What advice would you give to practitioners who are interested in a career in privacy?

MACKO: I came to the privacy bar mostly as an outsider. I've specialized in large-scale fraud investigations, securities cases, consumer protection investigations. And I found the privacy community to be remarkably welcoming and close-knit. Frankly, it shocked me, and I'm still not used to it. For anyone interested in privacy law, I'd encourage you to approach people you admire, leaders in the industry, and ask them for their advice about next steps. You'll be surprised by how helpful they'll be.

ENDNOTES

* Jennifer L. Mitchell is a Partner in the Los Angeles office of BakerHostetler, where she leads the Los Angeles, San Francisco and Orange County Digital Assets and Data Management practice. Jennifer has served on the Executive Committee of the Privacy Law Section of the California Lawyers Association since 2022. She focuses her practice on privacy compliance and advisory services. You can contact Jennifer at JLMitchell@ bakerlaw.com or learn more about Jennifer's background here: https://www.bakerlaw.com/professionals/jennifer-l-mitchell/

1. Mark Scott, *I have a plan to fix social media*, Digital Bridge, POLITICO (July 6, 2023, 1:30pm), https://www.politico.eu/newsletter/digital-bridge/i-have-a-plan-to-fix-social-media/.

Stay Ahead in Privacy Law with Our Premier CLE Courses!

Earn CLE credits and stay informed

Explore our extensive library of CLE's tailored to Privacy attorney's.

LEARN ANYTIME, ANYWHERE

SCAN HERE!

For More Information

calawyers.org/privacy

WRITTEN BY*

Kim Richardson

THE EVER-EVOLVING ROLE OF THE CHIEF PRIVACY OFFICER-TURNING CHALLENGE INTO OPPORTUNITY

INTRODUCTION

Data privacy is arguably the single most dynamic field of law. Privacy leaders are constantly managing a shifting and increasingly complex web of regulations, enforcement priorities, and litigation risks. Add to that the dizzying pace of technological advancements and you have a perfect storm of both exciting and daunting challenges, with the Chief Privacy Officer ("CPO") often tasked with charting the course and navigating the ship across what can be very murky waters.

Artificial Intelligence ("AI") is the latest example of a technological sea change that signals an inflection point that has the privacy profession rethinking and redefining its purpose, as privacy leaders are being tasked to take on broader data management responsibilities. A recent survey by the IAPP found that 69% of CPOs have added AI governance duties to their roles.[1] In fact, the leading global privacy professional organization, the IAPP, recently announced that it is officially expanding its mission beyond privacy to "define, promote and improve the professions of privacy, AI governance and digital responsibility globally."[2]

So then how do privacy leaders respond to all of this change? We do what we have always done. We learn, we adapt, we grow, we ride the waves as they come, and we thrive. Experienced privacy leaders are well-equipped to embrace this next phase of holistic data management. The history and evolution of our profession demonstrates why.

A BRIEF HISTORY OF THE CHIEF PRIVACY OFFICER ROLE (FROM ONE ATTORNEY CPO'S PERSPECTIVE)

Historically and today, the General Counsel's Office is the most common reporting line for CPOs, and many CPOs are attorneys.[3] In the early days (let's say, 2000-2010), unless you worked in a highly regulated industry (such as healthcare or financial), working in privacy as an attorney didn't feel much different from other attorney roles, outside of keeping up with the shifting regulatory landscape. In fact, many attorneys were adding privacy to a pre-existing broader role. Programs were in earlier states of maturity, and much of the day-to-day challenge involved working with business partners to ensure that privacy requirements were built into business products and initiatives. Concerns

around social media, mobile apps, and online tracking dominated the privacy headlines, along with news of large security breaches of well-known companies.[4] There were a limited number of sectoral federal laws to consider, and state laws designed to address specific issues were few and far between, outside of the developing data breach notification laws that started with California in 2002. The EU Directive was in play, but international data protection regulation and enforcement were somewhat limited on a global scale. IAPP reached its 10-year anniversary in 2010 with membership of 6,000.[5]

The following decade saw an explosion of privacy regulation and enforcement and corresponding growth and maturing of the privacy profession. Data breaches increased on a massive scale in both frequency and volume, eventually resulting in every US state and territory having its own breach notification law by 2018. The EU's General Data Protection Regulation (GDPR) took effect in 2018, adding a heightened level of rigor, accountability and enforcement risk to privacy compliance, with the potential of massive fines and extraterritorial reach sending a ripple effect across globe. The GDPR became the "gold standard" for comprehensive data protection regulation, and other countries and US states followed suit with comprehensive privacy laws modeled after GDPR in many respects. Transfers of European data to the US became increasingly challenging following the invalidation of the fifteen-year-old Safe Harbor Framework in 2015 and the ensuing path to the current Data Privacy Framework. US enforcement also intensified, with the FTC using its Section 5 unfair and deceptive trade practices powers to fill the gaps left by the US federal law's sectoral approach to privacy regulation. The 2011 Google Buzz consent decree marked the first time the FTC required a company to implement a comprehensive privacy program, which is now a standard feature of privacy consent decrees.[6] Add to this the proliferation of US class action litigation and what can one say other than, it's complicated! By the time the IAPP reached its 20-year anniversary, membership had surpassed 65,000. [7]

LOOKING TOWARD THE FUTURE OF THE CHIEF PRIVACY OFFICER

Through all of this change and growth, CPOs have adapted and taken on broader responsibilities. CPOs are already managing and/or partnering with cross-functional teams on privacy and data protection law, compliance operations, data security regulatory compliance and incident management, and data governance, ethics and strategy.[8] How then, can we leverage this varied experience as we move forward in the age of responsible AI governance?

GARNER STAKEHOLDER AND EXECUTIVE SUPPORT

While the importance of robust privacy programs may seem obvious in most organizations today, that has not always been the case. Privacy leaders have played an important role in bringing visibility to new issues that can have a profound impact on organizations. Just as the GDPR created a new era of enhanced rigor and accountability for privacy programs, the EU AI Act will likely have a similar effect on AI governance, being the first comprehensive AI regulation enacted, and carrying risk of fines and extraterritorial reach similar to that of the GDPR. Already we are seeing a flurry of guidance, frameworks, and proposed regulations emerging across the globe, and some limited instances of more targeted regulation.[9] The regulatory landscape is quickly forming, and CPOs are well positioned help organizations who wish to leverage AI understand the value of planning proactively for effective data governance.

CREATE THE GOVERNANCE TEAM

Privacy has always been a team sport. AI highlights the need for increased formalized cross-functional collaboration across various disciplines and skillsets, including legal, compliance, operations, technical and business. Data privacy, security and governance functions are already closely aligned with the issues and processes relevant for AI governance. Given the breadth of issues and potential risks that need to be considered, close partnership with technical and business teams will be especially critical. Ultimately, the structure will depend on the organization's existing governance mechanisms, the organization's role with respect to AI (e.g., a "provider" or "deployer" in EU AI Act terms) and the applicable use cases. CPOs can help to leverage existing relationships and structures to help ensure organizations take a holistic view toward data management that accounts for all of the diverse considerations that come to play with AI.

ADOPT A GOVERNANCE FRAMEWORK

Privacy programs are generally structured around a framework based on legal and industry standards that capture the key principles and elements required for effective compliance (e.g., GDPR, NIST, ISO). Privacy leaders can help drive adoption of an AI framework with core principles and controls designed to address the risks

and requirements of appropriate uses of AI. As most privacy regulations trace back to core privacy principles established by the Organisation for Economic Cooperation and Development ("OECD"), many countries have adopted the OECD AI Principles.[10] These principles form the basis of the governance framework that organizations can implement to support responsible AI, and bear similarity in some cases to principles applied in privacy frameworks, such as transparency, security, and accountability. And assuming that the EU AI Act is likely to become the gold standard for AI regulation, it may well serve as the optimal framework to use as a starting point as the regulatory landscape continues to unfold.

OPERATIONALIZE RISK MANAGEMENT

Like privacy programs, AI governance programs will need to implement policies and procedures to ensure that pre-existing and proposed uses of AI are identified and the right stakeholders are engaged to assess and mitigate risk. A good place to start is by leveraging data inventory and mapping work to identify AI uses and expand on those resources to collect additional information needed to support risk categorization. The EU AI Act takes a risk-based approach and determines obligations based on the risk of AI and the role of the organization.[11] The inventory and map can be used to assist with this initial categorization. Processes and tools used for Privacy Impact Assessments can be leveraged to collect additional necessary information to assess AI risk and ensure that risk mitigation measures are built into the AI implementation, similar to the privacy-by-design approach. The key will be finding ways to leverage existing risk management processes to coordinate efficient engagement across the various stakeholders who will need to be engaged for AI.

ENHANCE TRAINING AND AWARENESS

Last, but certainly not least, are training and awareness. Just as training and awareness are core pillars of privacy programs, education is critical for AI governance. One of the first requirements of the EU AI Act that will come into effect is the literacy requirement.[12] Privacy leaders can leverage existing training and awareness methods to educate members of their organizations who may engage with AI with broad and role-based education that takes account of evolving use cases.

CONCLUSION

CPOs have much to build on to embrace the new challenges posed by AI. Privacy is an important consideration for appropriate use of AI, and privacy programs have many building blocks that can be leveraged to support effective AI governance. Privacy leaders are accustomed to translating complex regulatory requirements into actionable and operationalized compliance programs. We are accustomed to wearing multiple hats and working cross-functionally in collaboration with the organizational stakeholders that need to be engaged for AI governance. While every organization will need to determine the best approach and structure for them, CPOs and teams will undoubtedly play an important role and have a prominent seat at the table as we embrace the challenges to come and the new opportunities for growth and leadership that these challenges bring.

ENDNOTES

* Kim Richardson is an accomplished Chief Privacy Officer and Legal Counsel with extensive experience building and leading privacy programs. Kim currently serves as VP Privacy, Chief Privacy Officer for Tandem Diabetes Care. Prior, Kim served as Chief Privacy Officer for Verily Life Sciences, and led Privacy at Mattel and Herbalife. Kim served as Vice President of Legal Affairs for Universal Studios Hollywood and held several positions at Disney, including Assistant General Counsel, Privacy. She also served as adjunct professor of Cybersecurity and Regulatory Compliance at Loyola Law School, Los Angeles. Kim received her J.D. from Harvard and her B.A. from UCLA, and holds several privacy certifications. https://www.linkedin.com/in/kim-richardson-esq-cipp-us-cipm-fip/

1. See IAPP's Organizational Digital Governance Report 2024. https://iapp.org/resources/article/organizational-digital-governance-report/

2. See IAPP Press Release, September 23, 2024. https://iapp.org/about/iapp-expands-mission-and-launches-cybersecurity-law-center/

3. See IAPP-EY Privacy Governance Report 2023. https://iapp.org/resources/article/privacy-governance-full-report/ See ACC Docket, Privacy Professionals Are on The Rise, February 9, 2022. https://docket.acc.com/privacy-professionals-are-rise

4. For example, see the Wall Street Journal's "What They Know" series. https://www.wsj.com/news/types/what-they-know. See Digital Guardian's The History of Data Breaches. https://www.digitalguardian.com/blog/history-data-breaches

5. See IAPP White Paper "A Call for Agility: The Next-Generation Privacy Professional" https://iapp.org/media/pdf/resource_center/IAPP_Future_of_Privacy_Final.pdf

6. See FTC press release "FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network." https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz-social-network

7. See IAPP-FTI Consulting Privacy Governance Report 2020 https://static2.ftitechnology.com/docs/IAPP-FTI+Consulting+-+2020+Privacy+Governance+Report.pdf

8. See IAPP's Organizational Digital Governance Report 2024. https://iapp.org/resources/article/organizational-digital-governance-report/

9. See IAPP Global AI Law and Policy and Tracker https://iapp.org/resources/article/global-ai-legislation-tracker/ and IAPP US State AI Governance Legislation Tracker https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker/

10. See OECD Privacy Principles https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 and OECD AI Principles https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 https://oecd.ai/en/ai-principles

11. See IAPP Top 10 operational impacts of the EU AI Act–Understanding and assessing risk. https://iapp.org/resources/article/top-impacts-eu-ai-act-understanding-assessing-risk/

12. See "Understanding the AI Act: AI Literacy Requirements and Compliance Strategies for Organizations," Ropes & Gray. https://www.ropesgray.com/en/insights/viewpoints/102jko5/understanding-the-ai-act-ai-literacy-requirements-and-compliance-strategies-for

WRITTEN BY

Jeewon Kim Serrato

CALIFORNIA VOTES TO ESTABLISH NEW PRIVACY LAW SPECIALIZATION

On December 13, 2025, the California Board of Legal Specialization (CBLS) voted to approve a new Legal Specialization in Privacy Law. This is the culmination of a process that the State Bar of California initiated in November 2022 by establishing a Consulting Group on the Establishment of a Legal Specialization in Privacy Law (Privacy Law Group). Appointed by the State Bar of California, the 13-member Privacy Law Group was tasked with studying the practice area to assess whether there is sufficient need and interest to create a specialty, as well as whether the area is sufficiently defined as to create a useful specialization. The Privacy Law Group determined that certification in this area of law is feasible and appropriate and presented draft certification standards for review by the CBLS and the State Bar Board of Trustees.

The next step will be the Board of Trustees meeting, scheduled for May 2025, where the recommendation will be reviewed. Following this, it will be posted for a 60-day public comment period. If all proceeds as planned, the final approval and adoption of the specialization will be considered and receive final approval at the subsequent Board of Trustees meeting in September 2025.

WHAT IS CBLS'S ROLE?

The CBLS administers the State Bar of California Program for Certifying Legal Specialists. This program was created by the California Supreme Court to promote attorney competence and provide consumers with an independent means to verify an attorney's qualifications. The legal specializations administered by the CBLS are the only programs by which attorneys can receive a designation as a specialist in an area of law. While there are other certifications available, this new Privacy Law Specialization is the only method by which privacy lawyers licensed to practice in California will be able to advertise themselves as a certified specialist.

With more than 225,000 attorneys, the State Bar of California is the largest state bar in the country. Nearly 170,000 lawyers actively practice law in California. The new privacy law specialization will have a significant impact on how attorneys in the U.S. think about privacy law specialization.

IS THERE A NEED AND DEMAND FOR A PRIVACY LAW SPECIALIZATION?

The Privacy Law Group presented to the CBLS and the State Bar agreed that privacy law is an area of law that can be defined and there is need and demand for privacy law specialists in California.

There were several discussions about the certification programs that are currently available in the market. While there are many other certification programs for privacy specialists, many are not exclusive to lawyers, therefore they do not signify

a specialization in privacy law, and they do not allow California-licensed attorneys to advertise themselves as a privacy law specialist due to the state bar rules.

This is the first time the CBLS has recognized a new legal specialty field in more than a decade. The Privacy Law Group discussed the rapid developments in privacy law that occurred in the last ten years. The fact that the California Lawyers Association (CLA) established a stand-alone privacy law section in 2020 and now has more than 1,200 members was discussed as one of the supporting factors for the CBLS to consider as it weighs whether there is need and demand for a specialization in privacy law.

WHAT IS PRIVACY LAW?

As part of the proposal and presentation to the CBLS, the Privacy Law Group discussed at length what it means to practice in privacy law. Over the course of a year, there were several discussions as to what is and is not privacy law. For example, the Group considered whether cybersecurity and artificial intelligence (AI) would be part of privacy. In the end, the Group considered the work privacy law practitioners currently engage in and sought to create a specialization that would be flexible enough to adapt over time to changes in the legal and regulatory landscape as well as emerging technologies that impact the legal practice.

Below is the list of continuing legal education topics in privacy law that were approved by the CBLS. Any attorney that receives the privacy law specialization would be expected to be a specialist in these areas:

- Frameworks and standards related to privacy and data security
- International privacy compliance and international data transfers
- Data subject rights
- Online privacy policies, notices and practices
- Children's privacy
- Financial privacy
- Health information privacy
- Educational privacy
- Employment privacy law
- Privacy laws governing advertising and marketing
- Law enforcement and privacy
- Emerging technology and privacy
- Cybersecurity and information security standards and requirements
- Data breach response, including breach notification requirements
- Privacy right of action

HOW CAN I BECOME A PRIVACY LAW SPECIALIST?

Once the proposal receives final approval from the Board of Trustees, California-licensed attorneys will be able to apply for the Privacy Law Specialization. While the exam is being developed, the CBLS approved an alternative process by which attorneys can receive the specialization. For the first two years after the specialization is established, licensees will be able to demonstrate that they have met the following Alternative to Exam Requirements and receive the Privacy Law Specialist designation.

Proposed Alternative to Exam Requirements in Privacy Law include:

- Submit a total of at least 150 points in Task and Experience Requirement.
- Supply evidence of at least 60 hours of continuing legal education or professional education from the topics in the Privacy Law Specialist exam specifications within the 5 years preceding the end of the two-year alternative exam period.
- Provide at least 5 peer references from attorneys, clients, or judges attesting to your privacy law qualifications.

The chart below describes how each applicant can meet the Task and Experience Requirement. For each section below in which you claim 20 or more points, you must also provide a brief narrative statement summarizing your experience in that area.

1. Provided substantive written legal advice or analysis regarding regulatory compliance with privacy laws. 5 points per matter. Maximum number of points in this category: 35 points.
2. Reviewed, drafted, or negotiated data privacy terms in contracts, including outsourcing/service provider agreements or other third-party contracts. 5 points per matter or transaction. Maximum number of points in this category: 35 points.
3. Provided substantive written legal advice or analysis regarding data sharing requests or counseling on cross-border data transfers and advised on privacy-related risks. 5 points per matter or transaction.

Maximum number of points in this category: 35 points.

4. Conducted data privacy due diligence involved in corporate transactions, including mergers and acquisitions, reorganization, bankruptcy, receivership, sale of assets, or transition of service to another provider. 5 points per matter or transaction. Maximum number of points in this category: 35 points.
5. Advised on policies, procedures, or processes relating to physical, technical, and administrative privacy and information security controls. 5 points per policy, procedure, or process. Maximum number of points in this category: 35 points.
6. Represented a party in litigation as its principal attorney on privacy issues where matters of privacy law are among the main contested issues. 5 points per separate litigation matter; 10 points per litigation matter if at least 500 hours are billed by the attorney on the case on privacy issues; or 15 points per litigation matter if at lest 750 hours are bills by the attorney on the case on privacy issues. Maximum number of points in this category: 65 points.
7. Represented a party in a government investigation as its principal attorney where matters of privacy law are among the main contested issues. 5 points per investigations matter; 10 points per investigations matter if at least 500 hours are billed by the attorney on the case on privacy issues; or 15 points per investigations matter if at least 750 hours are billed by the attorney on the case on privacy issues. Maximum number of points in this category: 65 points.
8. Acted as the principal attorney in devising and implementing the litigation strategy in connection with pending or threatened litigation where matters of privacy law are expected to be among the main contested issues. 5 points per litigation matter. Maximum number of points in this category: 35 points.
9. Acted as the principal attorney in devising and implementing a formal compliance program for a client following the entry of a court order, consent order, settlement, or other binding order or award against the client in any litigation or investigation matter where matters of privacy laws are among the main issues. 5 points per litigation or investigations matter. Maximum number of points in this category: 35 points.
10. Provided substantive written legal advice or analysis to conduct a data inventory or records of processing activities. 5 points per matter. Maximum number of points in this category: 35 points.
11. Provided substantive written legal advice or analysis to develop or implement external-facing privacy notices, statements or reports as required by privacy laws. 5 points per matter. Maximum number of points in this category: 35 points.
12. Provided substantive written legal advice or analysis on privacy issues for marketing, product, feature, or service delivery, such as implementing privacy by design or conducting privacy impact assessment. 5 points per matter. Maximum number of points in this category: 35 points.
13. Provided substantive written legal advice or analysis regarding data subject or consumer rights matters (e.g., access, deletion, opt-ins/opt-outs). 5 points per matter. Maximum number of points in this category: 35 points.
14. Led or participated in incident response or data breach investigation, including forensic analysis, root cause analysis, and remediation efforts, drafting, and reviewing incident reports and communications to stakeholders. 5 points per matter. Maximum number of points in this category: 35 points.
15. Assisted with breach notifications to regulators or affected individuals. 5 points per matter. Maximum number of points in this category: 35 points.

While the expectation is that attorneys in the private sector will most likely participate to earn the specialist designation, the Privacy Law Group recognized that the specialization should be available to recognize specialists who practice in government, in-house or other capacity. To the extent attorneys have experience that may not fit exactly into the listed requirements, the Task and Experience Requirements allow applicants to demonstrate substantial compliance with the requirements by submitting evidence of other experience. While the applicants need to show 150 points from the Task and Experience during the Alternative to Exam period, applicants for the specialization after the exam has been established will only need show 100 points.

HOW CAN ATTORNEYS PREPARE TO BECOME A PRIVACY LAW SPECIALIST?

The Privacy Law Specialist designation is not intended to show competence, but rather a high-level of expertise. For

attorneys interested in becoming a privacy law specialist, the CLA and other organizations provide excellent education resources. In addition to the legal education requirements, specialists will need to show that they are actively practicing in this area in order to meet the recertification requirements every five years.

You can subscribe to the email list to receive meeting notifications and updates from the Privacy Law Group here:

https://www.calbar.ca.gov/About-Us/Who-We-Are/Committees/California-Board-of-Legal-Specialization/Privacy-Law-Group.

HOW WILL THE PUBLIC BENEFIT FROM THE CALIFORNIA LEGAL SPECIALIZATION IN PRIVACY LAW?

California remains the 5th largest economy in the world since 2017, with a nominal GDP of nearly $3.9 trillion in 2023, according to the U.S. Bureau of Economic Analysis. On a per capital basis, California is the second largest economy in the world. California's tech workforce is over 1.5 million strong–more than the next two ranked states combined, according to the Computing Technology Industry Association. As emerging technologies like AI bring new legal issues to the forefront, the legal industry will be in need for specialists that can work with the tech industry in this exciting area of law.

Considering California's outsized economic power and its position as global leader in technological innovation, California attorneys will continue to play a significant role in establishing the rules and implementing compliance programs, as well as testing and challenging the industry's compliance with privacy expectations. This new Legal Specialization in Privacy Law will help the public search for and identify certified specialists in the area of privacy law. The Certified Specialist Search is available here: https://apps.calbar.ca.gov/members/ls_search.aspx

WRITTEN BY

Susan Rohol[1]

IS CALIFORNIA LEADING THE WAY ON AI OR JUST CAUSING CHAOS?

By the end of its 2023-24 session, the California Legislature passed, and Governor Gavin Newsom signed into law 17 artificial intelligence ("AI") bills. While California may have won the race for most U.S. state AI bills to become law, it is not the first jurisdiction to attempt to tackle these issues. The European Union's ("EU") AI Act and Colorado's AI Act both beat California to the punch and are arguably far more sweeping and comprehensive in their approach to AI regulation and risk assessment.

The variety in approaches begs the questions: How will this phase in the development of AI legislation play out? Will other U.S. states follow California and pass legislation that is sector- and/or use-case specific (i.e., targeted at digital replicas, sexually explicit deep fakes, use of AI in the health care sector, etc.)? Or will we see more U.S. states follow Europe and Colorado? Will U.S. states follow the trend we've seen with privacy laws, where jurisdictions are actively competing to demonstrate they are passing evermore restrictive regulations? Or will there be concern that this approach will hamper AI innovation? We have already seen Texas introduce legislation that is arguably broader and more sweeping than anything California, Colorado or Europe has passed into law—will other states follow suit? How will the new administration affect the federal response to AI regulation, and how will states respond? The one thing we can expect in 2025 is many AI bills, but in the meantime, here is a quick overview of the new laws in this space.

THE EU AND COLORADO'S COMPREHENSIVE APPROACHES

The EU and Colorado each have enacted a single comprehensive AI bill of general applicability that covers almost all AI systems, with a focus on classifying those systems based on the risk they pose to consumers and creating obligations on the developers or deployers of those systems based on that risk categorization.

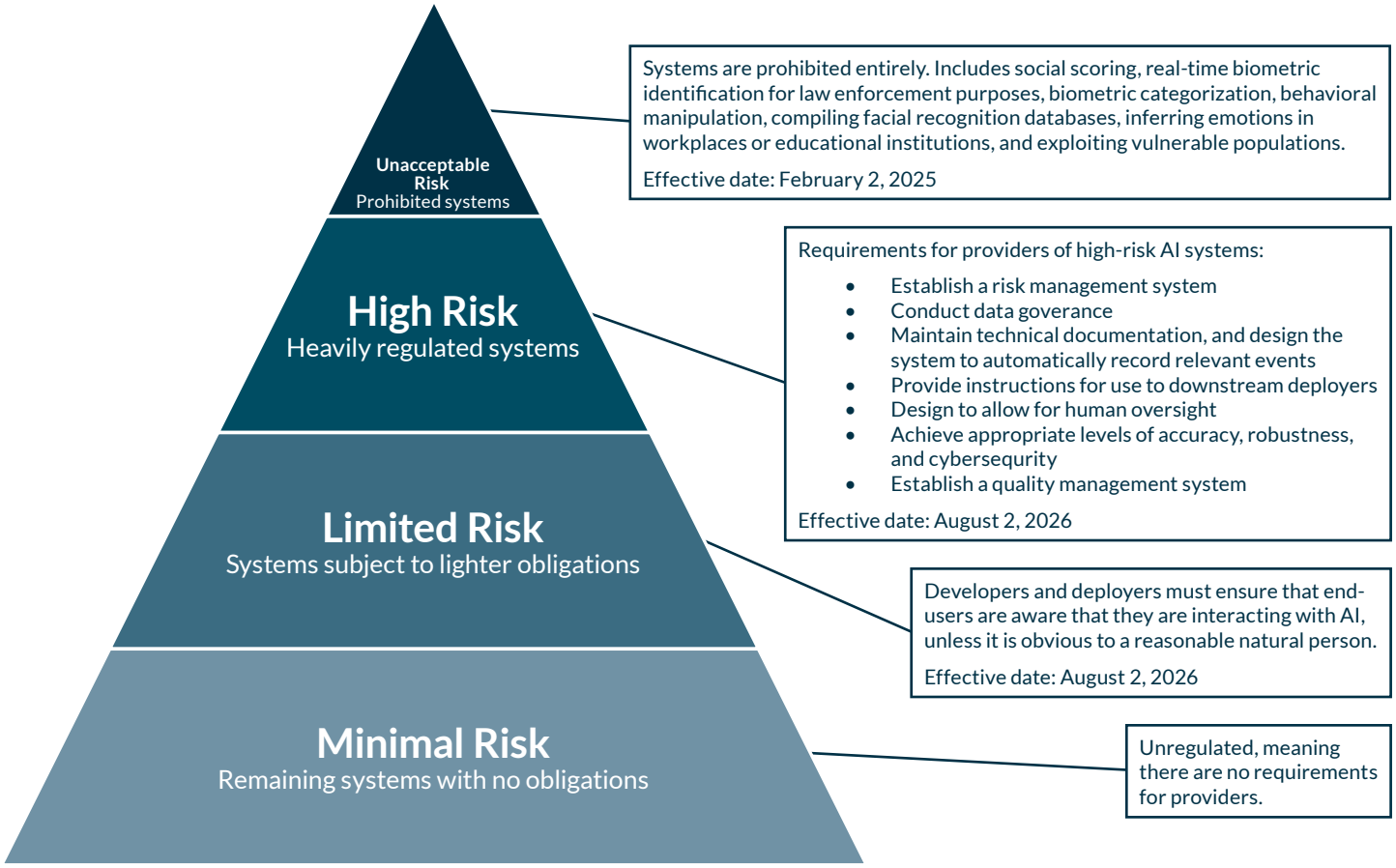
THE EU AI ACT

Arguably the most comprehensive approach to AI regulation is found in the European Union. It was initially proposed in 2021 (prior to the introduction of generative AI systems) and ultimately was enacted on March 13, 2024. The EU AI Act's[2] primary goal is to ensure that AI systems are safe and transparent. The European Commission found that the General Data Protection Regulation (GDPR)[3] did not adequately account for the changing technological landscape AI creates and the evolving dangers it poses, such as bias in systems or impacts to critical infrastructure.

The EU AI Act takes a risk-based approach to regulating the entire AI life cycle, from development to deployment, of different AI systems which operate in

the EU or provide services to users in the EU, and it applies irrespective of the industry in which the AI system primarily operates. AI systems are classified based on the risk they generate, and each tier corresponds to certain obligations. For instance, the EU AI Act outright bans certain "prohibited AI systems"–practices that are considered harmful or pose an unacceptable risk to people's safety, livelihoods, or rights (e.g., systems deploying subliminal or deceptive techniques or social scoring).[4]

EU AI ACT RISK TIERS



The EU AI Act focuses primarily on "high-risk systems."[5] It identifies eight types of systems that are deemed to be high-risk,[6] including biometric identification systems, critical infrastructure systems, and systems that determine access for admissions to educational or vocational training programs or evaluate employment or creditworthiness. High-risk systems are potentially exempt where the system is narrowly used, improves previously completed human activities, or involves decision-making that does not replace or influence a human assessment.[7] High-risk systems are also those that are used as a safety component of a product. These systems are required to undergo a third-party conformity assessment in order to place them on the market and are also subject to EU health and safety harmonization legislation.[8] Finally, an AI system will always be high risk if it performs profiling of persons.

While high-risk systems are permitted, they face a wide range of obligations in order to be developed and deployed in the EU, and require registration with the EU government prior to product release.[9] The broad exemptions that exist for high-risk systems will likely mean many companies do not classify their systems as high-risk in order to avoid registration and these onerous obligations.

The EU AI Act also addresses General Purpose AI Models ("GPAI")—i.e., those AI systems which can perform a wide array of generally applicable functions, such as image and speech recognition, audio and video generation, or pattern detection, and can be integrated into a variety of downstream systems, such as large generative AI models—placing obligations on these systems regardless of how they are placed on the market.[10]

The EU AI Act stipulates a right of natural and legal persons to lodge a complaint with a market surveillance authority, to explain individual decision-making, and to report instances of non-compliance. The EU AI office will supervise implementation and enforcement alongside national authorities. Penalties for non-compliance range from €35 million or 7% of worldwide annual turnover to €15 million or 3% of worldwide annual turnover, depending on the size of the violator and if the system is classified as a GPAI.

THE COLORADO AI ACT

Colorado followed in the footsteps of the EU, enacting its own law governing AI use based on risk.[11] Colorado's law predominantly regulates high-risk AI systems, which it defines as "any AI system that, when deployed, makes, or is a substantial factor in making, a consequential decision."[12] The Act creates duties for developers and deployers of high-risk AI systems to implement a risk management policy and conduct an impact assessment, using reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination.

It also creates transparency requirements for any consumer-facing AI systems, not just those that are high-risk. For instance, deployers and developers must make disclosures to inform users that they are interacting with an AI system (unless it would be obvious to a reasonable person), and they must notify users if a high-risk system is deployed to make a consequential decision about the user. Deployers and developers must also notify the Colorado Attorney General within 90 days if the deployed AI system has caused, or is reasonably likely to have caused, algorithmic discrimination. Violations of the Colorado AI Act constitute unfair trade practices, and punishments can include fines or injunctive relief.[13] Though not identical to the EU AI Act, with the EU focused more on risk management and Colorado favoring transparency and consumer rights, Colorado has similarly adopted the approach of one comprehensive piece of AI legislation.

THE CALIFORNIA APPROACH

California, on the other hand, has opted to legislate in a more piecemeal manner. Rather than adopting one comprehensive bill, it has created a patchwork of legislation, with each bill aimed at a different sector or identified issue. Seventeen bills on AI issues were enacted into law in the most recent legislative session, though many more were introduced. These new laws cover a wide breadth of matters,[14] ranging from implementing a uniform definition of AI in California law[15] to promoting election integrity by using AI to combat the spread of misinformation,[16] and legislating against deepfakes.[17] Several of these laws could, if adopted more broadly by other states, significantly impact the privacy landscape, including California's approach to digital replicas and training data disclosures.

Important to the privacy community is AB 1008,[18] a relatively short bill that packs a punch. This law amends the California Consumer Privacy Act ("CCPA") to clarify that personal information "can exist in various formats, including . . . artificial intelligence systems that are capable of outputting personal information." This addition means that any company utilizing AI must be aware that its AI system could generate information that California would consider subject to the protection of the CCPA (i.e., access, deletion, correction, and opt-out rights).

AB 2013[19] will also likely interest the privacy community. It implements a transparency requirement on developers[20] of generative AI systems before the system is made available to Californians by requiring certain disclosures regarding the underlying datasets used to train the generative AI system. Such disclosures to the developer's website must include: the sources or owners of the datasets; a description of the types of data within the datasets; and whether any of the datasets include data protected by intellectual property rights, were purchased or licensed, or include any personal information, amongst many other things. With its emphasis on data transparency–a core privacy principle–this law has significant implications and seems a likely candidate to be replicated by other states.

Another bill of note is AB 2602[21] which applies to any contract "between an individual and any other person for the performance of personal or professional services" to ensure performers can control use of their own digital replicas.[22] Though this bill is especially significant in California given the large entertainment industry, its effects are more wide-reaching, especially as other states could imitate its contents to apply to companies seeking to use digital replicas, such as in advertising, automated customer service bots, video games, or even something as mundane as corporate training videos.

California also enacted AB 3030[23] and SB 1120,[24] which require healthcare community members using generative AI to provide a disclaimer to patients, while also imposing numerous requirements, such as fair and equitable application of AI systems by healthcare service providers or

insurers. These bills are part of a larger legislative trend, as Utah has taken a similar approach and imposed transparency obligations on companies using generative AI, particularly in regulated industries like medicine.[25] This could be indicative that an industry-specific approach to legislating will become popular in an effort to better moderate how AI is used in higher-risk or regulated industries such as financial services, health care, and housing.

Notably, one heavily lobbied bill that would have adopted an approach much closer to the EU and Colorado approach did not make it past Governor Newsom. The Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (SB 1047)[26] would have imposed safety measures on large AI models to mitigate potential "critical harms" like the creation of biological or chemical weapons or a large-scale cyberattack against critical infrastructure. Unlike the rest of California's approach, this bill was not designed with a particular industry in mind and was, instead, more sweeping. Despite this, SB 1047 proved somewhat controversial, and while Governor Newsom agreed with state legislators that California cannot wait for a major catastrophe to occur before taking action to protect the public, he found that SB 1047, as drafted, was ineffective.[27] Because protecting against large-scale harms is a priority, the Governor has indicated that he will work on pushing forward a similar bill in the next legislative session.

LOOKING TO THE FUTURE

The one thing that is certain is that AI is not an issue that will be disappearing anytime soon, and we should expect more legislation in California, other U.S. states, and around the globe on this topic. Each of the new California laws, when taken individually, seems clear and doable. But it remains to be seen whether this volume of laws will address many of the critical issues that the public is concerned about. With such a decentralized approach, California will undoubtedly need to continue legislating and regulating in order to accommodate the gaps not yet covered through this patchwork of laws. The evolution of the landscape will also need to account for how these existing AI-related efforts are meant to work together and how compliance with them all is possible. Is such a system too abundant and variable? Or will it turn out to lead the charge in a new way of legislating AI? Time may tell.

ENDNOTES

1. With great thanks to Daniel Alvarez, Stefan Ducich and Alexandra Barczak for their contributions to this article.
2. 2024 O.J. (L 1698) [hereinafter the EU AI Act].
3. 2016 O.J. (L 119) 33.
4. *See* Ch. II Art. 5 of the EU AI Act.
5. See Ch. III Sections 2-5 for a comprehensive discussion of how the EU AI Act classifies and regulates high-risk systems.
6. The eight types are: non-prohibited remote biometric identification systems, biometric categorization, or systems used for emotional recognition; critical infrastructure; educational and vocational training used to determine access or admission to institutions, assess learning outcomes, or evaluate traits of individuals in employment; essential public or private services that are used to assess eligibility or creditworthiness; systems permitted for use by law enforcement; migration, asylum, and border-control management; and administration of justice, particularly voting. *See* Annex III of the EU AI Act.
7. *See* Ch. III, Section 1, Art. 6 of the EU AI Act ("[A]n AI system . . . shall not be considered to be high risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making . . . . [This] shall apply where . . . the AI system is intended to perform a narrow procedural task . . . is intended to improve the result of a previously completed human activity . . . is intended to detect decision-making patterns or deviations . . . and is not intended to replace or influence the previously completed human assessment. . . .").
8. *See* Ch. III, Section 1, Art. 6 of the EU AI Act.
9. These include establishing a risk-management system; training, validating, and testing data sets; keeping technological documentation up to date; deploying recordkeeping through automatic logging; ensuring transparency and human oversight; developing systems that achieve an appropriate level of accuracy, robustness, and cybersecurity; and conducting a fundamental rights impact assessment prior to deployment.
10. See Ch. V of the EU AI Act for a complete discussion of GPAI classifications and obligations. Requirements involve preparing and keeping up to date technical documents which must be provided to downstream providers integrating GPAI into their systems, performing fundamental rights impact assessments, implementing risk and quality management to assess and mitigate systemic risk, maintaining transparency in data used to train the model, informing individuals when they are interacting with AI, and ensuring AI generated output is marked and detectable as artificially generated.

11. S.B. 24-205, 74th Gen. Assemb., Reg. Sess. (Co. 2024).

12. *Id.* A consequential decision is a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of, education enrollment or opportunity, employment or employment opportunity, financial or lending service, an essential government service, healthcare services, housing, insurance, or legal services.

13. The Colorado Attorney General has exclusive enforcement authority, and there is no private right of action.

14. Note that two of the 17 bills apply only to the California government, so they are not discussed here.

15. A.B. 2885, 2023-24 Sess. (Cal. 2024) (defining AI as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.")

16. *See* A.B. 2355, 2023-24 Sess. (Cal. 2024) (requiring political action committees to disclose whether political advertisements have been generated or substantially altered by AI); A.B. 2655, 2023-24 Sess. (Cal. 2024) (requiring large online platforms, during specified periods leading up to elections, to (1) block materially deceptive content related to CA elections, (2) label certain additional content as inauthentic or fake, and (3) develop procedures for CA residents to report content that has not been otherwise blocked or labeled); A.B. 2839, 2023-24 Sess. (Cal. 2024) (prohibiting knowingly distributing, with malice, materially deceptive content within 120 days before an election in CA and, in certain circumstances, 60 days after an election). This last bill was found to be unconstitutional in October 2024 due to a lack of narrow tailoring.

17. *See* A.B. 1831, 2023-24 Sess. (Cal. 2024) (expanding the scope of existing child pornography laws to include matter that is digitally altered or generated by AI systems); S.B. 926, 2023-24 Sess. (Cal. 2024) (criminalizing the creation and distribution of deepfake pornography that reasonably depicts another person); S.B. 981, 2023-24 Sess. (Cal. 2024) (requiring social media platforms to establish channels for users to report sexually explicit digital replicas and temporarily blocking such material while the platform determines if permanent removal is required).

18. A.B. 1008, 2023-24 Sess. (Cal. 2024).

19. A.B. 2013, 2023-24 Sess. (Cal. 2024).

20. *Id.* A developer is any "person, partnership, state or local government agency, or corporation that designs, codes, produces, or substantially modifies an artificial intelligence system or service for use by members of the public."

21. A.B. 2602, 2023-24 Sess. (Cal. 2024).

22. It invalidates contracts that (1) allow for the creation of a digital replica to perform work that could have been done by the performer, (2) fail to specifically describe the intended users of the digital replica, and (3) were negotiated without legal and/or union representation.

23. A.B. 3030, 2023-24 Sess. (Cal. 2024).

24. S.B. 1120, 2023-24 Sess. (Cal. 2024).

25. S.B. 149 Artificial Intelligence Amendments, §§ 13-2-12(1)(a)-(c), 13-2-12(5) (Utah 2024).

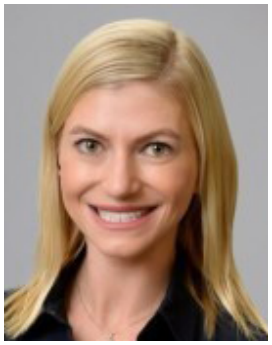
26. 3 S.B. 1047, 2023-24 Sess. (Cal. 2024)

27. Governor Gavin Newsom, SB 1047 Veto Message, Office of the Governor (Sept. 29, 2024) https://www.gov.ca.gov/wpcontent/uploads/2024/09/SB-1047-Veto-Message.pdf. The Governor cited the following reasons for his veto: (1) it only focused on the most expensive and large-scale models, and could give the public a false sense of security about controlling AI; (2) it did not take into account whether an AI system was deployed in high-risk environments, involved critical decision-making, or used sensitive data; and (3) it was not informed by an empirical trajectory analysis of AI systems and capabilities.

STATE PRIVACY LAW IN 2025-WHAT TO EXPECT

WRITTEN BY*

Justin Yedor



Taylor Bloom

Things happen quickly in the world of data privacy. With new laws being enacted, regulations continuing to develop and enforcements an ongoing reality, it can be difficult to track all the recent developments in U.S. comprehensive privacy regulation. This article will provide an update on the laws that will be in effect as of January 2025 and summarize important trends to be aware of.

By April of 2024 nearly 20 percent of U.S. consumers had rights under their states' privacy laws. And by October of 2024 that number had increased another 10 percent. By January 2025 it will be 40 percent, and nearly 50 percent by January 2026. Even in the absence of a federal privacy law, data privacy regulation is starting to become the norm across the country.

NEW STATE PRIVACY LAWS

Throughout 2024 we continued to see states passing similar but not identical privacy laws. In 2024, seven state legislatures (Nebraska, New Jersey, New Hampshire, Kentucky, Maryland, Minnesota, and Rhode Island) passed comprehensive privacy laws, which will take effect over the next couple of years. The good news for those working to comply is that a model does seem to be developing, at least in terms of the laws' core requirements. For example, many of the laws passed to date are loosely based on the Virginia or Connecticut laws, with similar rights and requirements relating to notices, opt-outs, contracts, and the rights to access, delete and correct personal data. Nonetheless, it would be overly simplistic—and risky—to treat compliance with one of these laws as sufficient to cover all of the others. While all share common goals of consumer protection, transparency, increasing control over personal data, and limiting targeted advertising, there are significant differences among each of these laws related to the right to opt out of profiling, recognition of browser-based opt-out preference signals, and data protection impact assessments (DPIAs), among other topics. There are also significant differences in the thresholds under which companies may become subject to a state's privacy law.

Among the new laws taking effect in January, Delaware and New Hampshire have much lower thresholds than what we typically see—processing the personal data of 35,000 consumers will be enough to bring a business in scope. Iowa and New Jersey use the 100,000-consumer threshold that we are accustomed to from Colorado, Connecticut, and Virginia. Nebraska's privacy law, on the other hand, does not rely upon revenue or data processing volume for applicability. Instead, Nebraska's law—like the Texas Data Privacy and Security Act—applies to persons that conduct business in Nebraska or produce products or services consumed by Nebraska residents and are not small businesses as defined by federal law.

UPDATES TO EXISTING STATUTES AND REGULATIONS

Meanwhile, even states that already had privacy laws in effect—such as California and Colorado—recently passed bills

modifying those laws to address new developments in technology such as the processing of neural data, biometrics, and artificial intelligence. For now, these statutory updates are likely to have only a modest impact on most businesses' compliance efforts, though they may prove to be more significant in years to come if computer chip implants and wearable brain activity monitors become more widespread.

In March 2023, the Colorado Attorney General (AG) released regulations under the Colorado Privacy Act describing detailed requirements and examples relating to topics such as notices, privacy rights requests, browser-based opt-out signals, DPIAs, loyalty programs and profiling. Now the Colorado AG is back at it, having recently announced proposed draft amendments to the Colorado Privacy Act Regulations that would create a process for issuing opinion letters and interpretive guidance, require special notices for biometric identifiers, and clarify some sections of the existing regulations. This new rulemaking is currently underway.

On March 29, 2023, the California Office of Administrative Law approved the first set of regulations promulgated by the California Privacy Protection Agency (CPPA) under the California Privacy Rights Act (CPRA) amendments to the California Consumer Privacy Act (CCPA). These regulations followed extensive formal and informal rulemaking that began in 2021 but still did not address all of the topics designated for rulemaking under the CPRA. In the fall/winter of 2023, the CPPA published five additional sets of draft rules addressing cybersecurity audits, risk assessments, automated decision-making technology (ADMT), exceptions for insurance companies and still further updates to the existing CCPA regulations. Since then, the proposed regulations governing ADMT proved to be a source of much debate among the CPPA Board, stalling the entire rulemaking package from advancing into the formal rulemaking process.

When the CPPA Board met again on November 8, 2024, some members of the Board and many members of the public continued to raise issue with the ADMT Regulations. However, despite these apparent misgivings, a majority of the Board voted to move forward into the formal rulemaking process with the five sets of proposed CCPA regulations, citing (a) the further delay that would be caused by sending the rules back to the CPPA for further pre-rulemaking revisions, and (b) the hope that the formal rulemaking process would lead to appropriate revisions to the rules. At this point, we do not expect final regulations until at least mid-2025.

The Board also voted to give final approval for new regulations covering data broker registration requirements under the California Delete Act. The new data broker requirements diverge from prior requirements in several ways, and include a narrowed definition of a "direct relationship," which could sweep many more businesses into the concept of a data broker. They also include a 1550% increase to the data broker registration fee, which the CPPA intends to use to fund its new "Deletion Request and Opt-Out Platform" (DROP). The DROP is intended as a one-stop mechanism for California residents who wish to delete their personal information from data broker files. It is expected to open to consumers on January 1, 2026, with data brokers required to access the platform and start processing consumer deletion requests beginning August 1, 2026.

EXPANDING ENFORCEMENT

With the influx of new privacy laws, it is more important than ever to have a strong compliance posture going into 2025. Regulators from an increasing number of states are launching investigations, monitoring consumer complaints, and actively addressing privacy grievances. AGs are also actively working together and have expressed that they often receive referrals from other agencies. Generally, companies should approach investigations collaboratively to prevent escalation and maintain open dialogue with regulators, but the best strategy for mitigating enforcement risk remains actively focusing on compliance.

With so many new developments afoot, 2025 is looking to be another busy year in the world of U.S. data privacy.

ENDNOTE

* Justin T. Yedor is a Partner in the Los Angeles office of BakerHostetler. Justin partners with clients to develop creative solutions to data privacy challenges. He is a thought leader on California privacy law and a go-to advisor on the California Consumer Privacy Act and the next wave of U.S. state privacy laws taking effect across the country. You can contact Justin at jyedor@bakerlaw.com or learn more about his background here: https://www.bakerlaw.com/professionals/justin-t-yedor/

Taylor A. Bloom is a Partner in the Orange County office of BakerHostetler. Taylor has significant experience operating at the intersection of law, technology and business, with a keen focus on both U.S. and international data protection, data privacy and governance. You can contact Taylor at tbloom@bakerlaw.com or learn more about her background here: https://www.bakerlaw.com/professionals/taylor-a-bloom/

WRITTEN BY*

Ben Isaacson

WAKE NOW, DISCOVER THAT YOU ARE A DATA BROKER

California's SB 362 'Delete Act' is now just one of numerous U.S. laws specifically regulating data brokers, in addition to recent FTC consent decrees with companies engaged in various aspects of data licensing. This article explores the many ways in which companies may unknowingly qualify as a data broker, as well as other state and federal data broker compliance requirements or FTC guidance.

U.S. STATE LAWS UPDATE

States: There are now five (5) states with laws specifically regulating data brokers. While they are quite similar, there are nuances with definitions, exemptions, and enforcement. To quickly summarize, they are (in order of enactment):

- **Vermont:**[1] Requires data brokers to register with the state, implement specific data protection and security standards, and incur penalties of up to $50/day for non-registration. Its most unique aspect is that a data broker security breach may be deemed an 'unfair or deceptive practice' under their Consumer Protection Act and lead to specific damages.
- **California:**[2] Requires data brokers to register with the state, report annual data subject rights metrics, undergo a future third-party audit, and incur penalties of up to $200/day for non-registration. Its most unique aspect is the introduction of a 'Deletion Mechanism' to be created by the California Privacy Protection Agency by August of 2026 to effectuate consumers' state-wide requests to delete (and/or be opted-out) of data broker activities. *See the California Regulatory Update below for more information.*
- **Nevada:**[3] No data broker registration is required. The scope of the law is limited to businesses whose 'primary' activity is licensing third-party data, and only requires the designation of an address to collect and honor 'Do Not Sell' requests. Its most unique aspect is that it grants data brokers a reprieve for their 'first failure' to honor any such requests.
- **Texas:**[4] Similar to NV, it is limited to businesses whose 'principal source of revenue' is licensing third-party data. It requires data brokers to register with the state, implement specific data protection and security standards, and incur penalties up to $100/day for non-registration. Its most unique aspect is its requirement that a data broker post a 'conspicuous notice' on its websites stating that it is a data broker as specified by the TX secretary of state.
- **Oregon:**[5] Requires data brokers to register with the state and incur penalties of up to $500 per day for non-registration. It exempts

businesses licensing data associated with 'publicly available business professionals.' Its most unique aspect is its intersection with the Oregon Consumer Data Protection Act[6] which includes a stipulation as part of data subject access requests for data sellers to provide a 'list of specific third-parties' who received the data subject's personal data.[7]

FEDERAL LAWS & FTC UPDATE

FCRA: There's a misnomer that data brokers have historically been unregulated under federal law, as the Fair Credit Reporting Act (FCRA) has effectively regulated the collection and licensing of data used for broadly defined 'consumer reports' for more than fifty years.

PADFA: In addition to the FCRA, there is now another federal law specifically governing data broker activities which is entitled the 'Protecting Americans' Data From Foreign Adversaries Act of 2024' (PADFA).[8] The law prohibits data brokers from licensing 'personally identifiable sensitive data' to 'foreign adversaries' and includes the following key definitions:

- A 'foreign adversary' is any entity 'controlled' by a foreign adversary country or a business with a controlling interest from residents of foreign adversary countries as per ECFR § 791.4[9] (e.g., Iran, China, Russia, North Korea, others).
- A 'data broker' is "an entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider."
- The list of 'personally identifiable sensitive data' attributes is quite broad, and includes health-related conditions or treatments, race, ethnicity, religion, *online behavioral activities*, and precise geolocation information.

PADFA does not specify a 'knowing' requirement, so every data broker must complete 'beneficial ownership' due diligence on every one of their data licensees to ensure compliance. PADFA includes a broad exemption for intermediaries acting as 'service providers' on behalf of data brokers, and is exclusively enforced by the FTC.

Federal Trade Commission (FTC): While FTC consent decrees are not considered law or regulation, the FTC recently settled cases with entities engaged in data licensing that are quite novel in many ways, with some serious restrictions on these entities use of data, including:

1. **FTC vs X-Mode Social/Outlogic:**[10] The FTC asserted that X-Mode sold 'raw precise geolocation data' without receiving any 'informed consent', and did not filter out any 'sensitive' locations such as medical facilities. The FTC's assertion of a lack of consent was irrespective of X-Mode's contractual terms with their licensors requiring them to obtain such consent on X-Mode's behalf, as well as the fact that mobile operating systems require user consent prior to an app collecting GPS information. As part of the agreement, X-Mode was forced to delete all previously collected precise location data collected without 'informed consent' and further requires X-Mode to provide consumers upon request with 'the identity of any individuals and businesses to whom their personal data has been sold or shared.'
2. **FTC vs InMarket Media:**[11] Similar to X-Mode, this settlement was due to the FTC's assertion that InMarket licensed precise location data with a lack of 'informed consent' from end users. The agreement prohibits InMarket from *"selling, licensing, transferring, or sharing any product or service that categorizes or targets consumers based on sensitive location data."* A unique aspect of this case beyond the FTC's novel classification of InMarket's 'places' location data as 'sensitive' is the fact that some of InMarket's data was collected through their own mobile apps with their own proprietary rights to license this data, in addition to these apps seemingly complying with mobile operating systems app store requirements for acquiring consent in order to collect precise location information.

DIFFERING DATA BROKER DEFINITIONS

As noted, U.S. state and federal laws have slightly different definitions of 'data brokers' with these notable differences:

1. **Indirect relationship.** All data broker laws include the terms 'with whom the business [or person] does not have a direct relationship' or 'did not collect directly from the individual'. However, as noted above in the case of FTC vs InMarket, this consistent applicability to 'third-party data' did not stop the FTC from asserting claims against InMarket who licensed data they collected directly from individuals through their own apps. As a result, even though data broker laws may exempt direct collection 'first-

party' data licensors, other laws or regulations may yet still be applicable to companies licensing data they collect directly from end users.

2. **Knowledge.** California and Vermont hedge their data broker definitions such that a data broker must 'knowingly' collect and sell consumer data, while the other states and federal laws do not include any such 'knowledge' requirement.
3. **Primary purpose.** Nevada and Texas both narrow the scope of their laws to entities (and in Nevada's case 'or individuals') where their revenue is predominantly made through third-party data licensing. California also has a threshold to meet the definition of data brokers, requiring that they must be 'businesses' as defined under the California Consumer Privacy Act (namely, a data broker must: 'derive 50 percent or more of its annual revenues from selling or sharing consumers personal information' or sell or share the personal information of 100,000 or more (California) consumers or households). The other states (VT, OR) and federal laws have no such 'threshold' so all data brokers are in scope regardless of their revenue allocation or quantity of state-specific data sold.
4. **Corporate and affiliate alignment.** California's definition of 'business' allows for affiliates or subsidiaries to be deemed data brokers without implicating a parent company, affiliate or subsidiary. In addition, both Oregon and Vermont include the terms 'business or units of a business' which narrows the scope of data broker applicability to be a line of business, divisions or affiliates under the same corporate umbrella. Companies with a 'data broker product' may wish to spin the entity into its own business entity in order to avoid running afoul of these state requirements.
5. **Households not included.** California is the only state that includes the term 'household' in its prescriptive requirements under the CCPA, but it chose not to extend any such specificity in its data broker definition. No other U.S. states extend their definition of personal information or data broker registration requirements exclusively to household-level data (even if few data brokers operate exclusively with this data).

CLASSIFYING DEFINITIONAL CATEGORIES

In the Federal Trade Commission 2012 report 'Protecting Consumer Privacy in an Era of Rapid Change' data brokers are defined as *"companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."*[12] This is a great starting point to classify the categories of data brokers, as there are numerous use cases in each category that could result in businesses inadvertently being categorized as data brokers.

1. **Verifying an individual's Identity.** While most identity-related data broker activities, such as credit reporting, background check services, or 'people-search' websites are regulated under the FCRA and exempt from certain data broker laws, there are many other identity-related services that are outside the scope of the FCRA. Specifically, companies that may be in scope include:

    - 'Identity resolution' businesses who attempt to validate the accuracy or deliverability of a first-party's data through the use of third-party data sources. The intermediaries providing these services typically source the third-party data themselves, and are not 'instructed by' the first parties to specifically license this data on their behalf. The intermediaries also combine disparate data sources in order to provide potentially new information directly to the first party, which is akin to brokering a third-party list for the first party's use.
    - 'Device graphing' business who match multiple identifiers associated with the same user, device or household in order to assist a first party with identifying, targeting or measuring their marketing or other business activities. Again, these services rely on third-party data and are effectively 'appending' new identifiers to existing records.

2. **Differentiating Records.** In marketing parlance, this can be referred to as 'data appending.' Any businesses that sources third-party data for the purpose of appending it to a first-party's personal data may be in scope as a data broker. These licensing activities typically involve appending demographic, psychographic, or behavioral data to augment a business's existing customer identifiers for direct marketing, programmatic, or addressable advertising, customer communications, personalization, measurement, and market research.

The following categories of companies may inadvertently now be defined as data brokers:

- Advertising or marketing agencies where they license third-party data for all of their clients, rather than being instructed by a client to specifically license data on their behalf. The contractual terms of these 'written instructions' to direct agencies to procure third-party data must be transparent, and ideally reference the specific data licensor(s).
- Advertising services that embed third-party data into their applications, notably those that include 'interest-based' categories from 'across websites or apps.' By selling interest-based attributes, these businesses are prohibited from being considered 'service providers' under the CCPA for those data services. Further, if these businesses enable the interest-based or licensed demographic data to be available for use by any other business (and not just the first party who enabled the 'retargeting' activity), then the business will be classified as a data broker.

3. **Financial and health-related services.** California and other state laws exempt entities regulated under the Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA). However, there are situations where data collected for, or in association with, a GLBA or HIPAA regulated company will still be subject to state or federal data broker requirements, namely where a covered entity works with an intermediary to engage in 'lead generation' activities such as sponsoring sweepstakes or events in conjunction with a partner who then licenses the data to third parties. Just because the 'covered entity' financial or health services brand is associated with the collection of the information does not mean that the 'lead generation' intermediary collecting and licensing the information is exempt from compliance with data broker requirements.
4. **Marketing services.** The term 'marketing' can incorporate any third-party data use activities that extends beyond 'targeting.' Companies serving as intermediaries between marketers and data providers can easily become data brokers if they are not 'following specific instructions' with procurement of third-party data. Some of the categories that may be in scope include:
   - Market research providers who may license 'panels' of survey respondents and/or their responses for use by businesses or other market research providers where they did not collect the original survey respondent information.
   - Measurement providers who license and combine third-party data in order to measure a business's brand, advertising or marketing performance where the first-party data did not provide them with specific instructions, similar to the 'agency' reference above.
   - 'Personalization' applications such as where a SaaS platform or other service combines specific behaviors or data insights (with or without third-party data) in order to provide the results to unrelated third parties. For example, an email service provider (ESP) may collect the days and time that specific recipients click on links in email ads, and then optimize any of their clients' email campaigns to automatically target those same recipients at the optimal day/time. In this example, the ESP is licensing email-specific behaviors from across multiple businesses to unrelated third parties for their own use.

A Mixed Category: Business-to-Business Services. Each state treats 'business professional' information differently. California specifically requires companies licensing business professional data to comply with its data broker law, while Vermont and Oregon's laws as well as PADFA specifically exempts 'publicly available' business professional data. As a result, determining data broker compliance for business professional data requires careful diligence on the source of any such data, and whether a 'publicly available' exemption may apply.

CALIFORNIA-SPECIFIC REGULATORY UPDATE

In a board meeting on Friday, November 8, the California Privacy Protection Agency (CPPA) voted[13] to adopt regulations[14] under the California 'Delete Act'. These regulations update the data broker registration process, and various applications of the law to distinct types of data brokers.

REGISTRATION UPDATES

While most of the registration process and form will be unchanged from 2024, the regulations include the following

additional requirements and clarifications. To summarize, data brokers must:

- Pay the annual registration fee with a credit card (with some exceptions).
- Uniquely register each business that operates as a data broker regardless of status as a parent company or subsidiary (i.e. a parent company of a registered data broker does not need to register as well as the subsidiary unless they, too, operate as a data broker).
- Provide the CPPA with a point of contact - this will not be posted on the public registry.
- Sign registrations under penalty of perjury to affirm that the information submitted on the registration form is true and correct.

EXPANDING THE SCOPE OF THE LAW TO ANY 'INDIRECT' DATA SALES

1. **Three year 'statute of limitations' on a 'direct relationship'.** The definition of 'direct relationship' embedded in SB 362's definition of 'data broker' now includes where *"a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services* ***within the preceding three years****."* In other words, any first party that 'sells' or licenses data will need to register as a data broker for data that is licensed following three years after the initial collection date. This could potentially be mitigated with 'any' record of an interaction or other relationship activity, including a website visit or email click-through. However, theoretically this could mean that a first party that licenses their data will be required to 'audit' their own databases to ensure that they have engaged with these individuals within the prior three year period or else be forced to either suppress those old identifiers, or register as a data broker.
2. The CPPA also added the following statement to their modified definition of 'data broker' to include the following: *"**A business is still a data broker if it has a direct relationship with a consumer but also sells personal information about the consumer that the business did not collect directly from the consumer."*** This language can be interpreted quite broadly, and could include the following potential scenarios:

    - A business licenses third-party data (or collaborates with a joint marketing partner), such as appending demographic or behavioral information to its first-party data, and then enables that appended first-party data to be used for third-party data licensing or addressable advertising. This is a common historical practice with catalog mailer 'coops' where they share postal lists of their customers with other cataloguers, but append demographics as part of the advertisers list selection. Even though the cataloguer may only be licensing their own first-party customer data, they may be deemed 'data brokers' if third-party data is also available for list selection.
    - A business uses a third-party 'identity resolution' service to enable addressable or targeted advertising on its own media, or in conjunction with third-party media buying. Identity resolution commonly matches additional third-party identifiers with a first-party identifier to expand the scope of matching with advertiser information or to reach an individual across multiple devices. If the media provider 'sells' the capability to reach these indirectly collected identifiers, then the business may be deemed to be a 'data broker.'
    - **Could this definition even apply to the entire 'interest based' or 'cross contextual behavioral' advertising industry?** Most website publishers do not 'directly' collect the attributes associated with website behaviors, but rather rely on third parties. While the website may 'authorize' the collection and use of this information for their own media sales, the fact is that another 'third party business' will be the entity actually collecting, managing, and selling that behavioral information. As a result, it is conceivable that when a website publisher also 'sells' access to behavioral information for ad targeting on their own website that they, themselves, did not collect, then they could be deemed to be a 'data broker'.

As for next steps, the regulations are sent to the Office of Administrative Law for final approval. If approved, the regulations will go into effect by the start of the January 2025 registration period.

HOW TO REGISTER IN 2025

The registration period begins January 1, 2025 and is expected to be completed by January 31 for existing data

brokers that reach the 'business' threshold. Once the registration form is submitted on the CPPA website, data brokers will be provided a link to a portal where they can pay the registration fee via credit card and complete their registration. Data brokers will also be required during the 2025 registration period to submit their 2023 consumer privacy rights requests metrics - these are the same metrics that were required to be published in data broker privacy policies in July 2024.

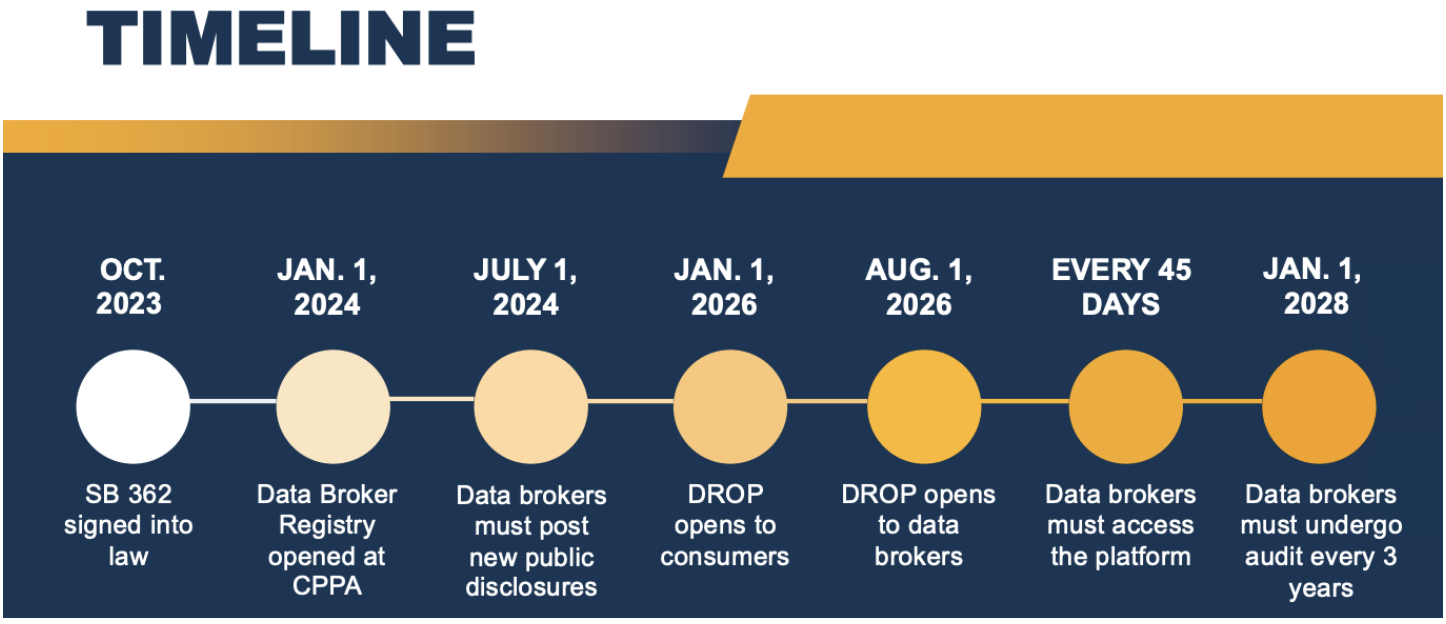
If data brokers have not registered by January 31, 2025, they may be liable for administrative fines for each day the data broker was unregistered. *(More below on recent enforcement actions.)*

Very Important Update: On November 8th, the Agency Unanimously Approved A Measure To Increase The Annual Data Broker Registration Fee To $6,600

In addition to the regulations, the CPPA voted and approved a measure to increase the annual data broker registration fee from $400 to $6,600 (plus associated third-party fees for processing electronic payment). The steep increase is due to the fact that the Delete Act statutorily requires the annual data broker registration fees to pay for the Delete Act's one stop mechanism enabling consumers to submit a single opt out or deletion to all registered data brokers. The CPPA has titled this mechanism the Delete Request and Opt-Out Platform (DROP). The Agency must have DROP ready and operable by January 1, 2026, and starting on August 1, 2026, data brokers must access DROP at least every 45 days (see timeline provided by the Agency below).

Prior to the November meeting, the CPPA put out a Request for Information (RFI) seeking preliminary information from potential vendors to create and operate DROP. The Agency received bids with a significant range of costs from $800,000 to $12,000,000. From these informal initial responses, and before ever putting out an official Request for Proposal (RFP) for more concrete costs, the Agency concluded that the budget should be $4,400,000 for 2025 and voted unanimously to approve the $6,200 registration fee rate increase to account for the $3,500,000 necessary to supplement their existing budget. They now expect that the 527 registered data brokers will each pay the significantly increased fee beginning January 1, 2025 in order to collect the necessary funds to use towards creating the DROP. In addition, the Agency has confirmed the following key details:

1. Regardless of the final operating expenses associated with the DROP, the current fee will not increase within the 2025 calendar year, nor will data brokers receive a pro rata refund if the DROP costs less than the anticipated budget. This is also seemingly regardless of whether there is a dramatic increase or decrease in 2025 registrations.
2. The CPPA orally noted that they expect to adjust the registration fee again for 2026 once DROP is created, but did not indicate whether any budget overages would carry into the 2026 registration fee, nor how they would determine a 'maintenance budget'.
3. As noted below, on Nov 14, 2024, the CPPA announced it had reached settlements with two data brokers who had failed to register, and that they received approximately $69,800 in revenue



that, theoretically, should be applied to funding the DROP.[15]

IN A TARGETED ENFORCEMENT SWEEP, THE CPPA FINED TWO UNREGISTERED DATA BROKERS

On October 30, 2024, the CPPA's enforcement division announced an investigative sweep of unregistered data brokers. In the November 8th Agency board meeting, the Agency voted unanimously to approve settlements with two data brokers, Growbots, Inc. and UpLead LLC, for failing to register and pay the annual registration fee. The companies will pay their registration fees as well as fines of $200 per day for failing to register by the deadline. Growbots will pay $35,400 for allegedly failing to register between February 1 and July 26, 2024; UpLead will pay $34,400 for allegedly failing to register between February 1 and July 21, 2024. In addition to the fee and fines, both companies agreed to injunctive terms, including agreeing to pay the CPPA's attorney fees and costs.

CONCLUSION

With disparate state laws, a new federal law, new California regulations and recent relevant FTC consent decrees, it is increasingly difficult for companies engaged in sourcing and licensing third-party data to avoid being defined as data brokers. While the compliance complexities vary, the common thread is that data brokers are being forced to be more transparent about their existence, process significantly more privacy rights requests, and be subject to new regulators with specific statutory penalties for non-compliance. More importantly, many businesses that have regularly licensed third-party data and thought they were 'service providers' on behalf of their clients now have the eyes of the world upon them and may need to modify their business practices.

ENDNOTES

* Ben Isaacson is a Principal at In-House Privacy, Inc. Ben has been a privacy practitioner since 1996, a CIPP since 2005, and currently serves as a fractional privacy officer, privacy counsel and consultant to a diverse set of clients ranging from early-stage tech startups to public companies with a strong emphasis on adtech/martech and data licensing. www.InHousePrivacy.com

1. Vt. Stat. Ann. tit. 9, ch. 062 (2024). https://legislature.vermont.gov/statutes/chapter/09/062.
2. S.B. 362, 2023-2024 Leg., Reg. Sess. (Cal. 2024). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362.
3. Nev. Rev. Stat. ch. 603A (2024). https://www.leg.state.nv.us/nrs/nrs-603a.html.
4. Tex. Bus. & Com. Code § 509 (2024). https://statutes.capitol.texas.gov/Docs/BC/htm/BC.509.htm.
5. H.B. 2052, 2023 Leg., Reg. Sess. (Or. 2024). https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/HB2052/Enrolled.
6. S.B. 619, 2023 Leg., Reg. Sess. (Or. 2024). Section 3(1)(a)(B) https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled.
7. *Id*. Section 3(3) This requirement is 'at the controller's option' and does not require the disclosure of 'trade secrets.'
8. H.R. 815, 118th Cong. (2024). https://www.congress.gov/118/bills/hr815/BILLS-118hr815enr.pdf.
9 15 C.F.R. § 791.4 (2024). https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-E/part-791/subpart-A/section-791.4.
10. FTC Order Prohibits Data Broker X-Mode Social/Outlogic from Selling Sensitive Location Data, Fed. Trade Comm'n (Jan. 2024). https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.
11. FTC Order Will Ban InMarket from Selling Precise Consumer Location Data, Fed. Trade Comm'n (Jan. 2024). https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data.

12 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

13. https://cppa.ca.gov/announcements/2024/20241108_2.html
14. https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf
15. https://cppa.ca.gov/announcements/2024/20241114.html

PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION
400 Capitol Mall, Suite 650
Sacramento CA, 95814

CALIFORNIA LAWYERS ASSOCIATION
THE BAR ASSOCIATION FOR ALL CALIFORNIA ATTORNEYS
CALAWYERS.ORG | @CALAWYERSORG