Coblentz
Patch Duffy
& Bass LLP

# 2025 Mid-Year Privacy Report

## A Comprehensive Look at New Developments in Data Privacy Laws

**Coblentz Patch Duffy & Bass LLP**
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com

**Summer 2025**

# Contents

# Introduction

In 2025, privacy and AI regulation have moved from the sidelines to the center of business risk and strategy. U.S. states are rapidly enacting a patchwork of privacy laws, with new AI laws emerging and expected to increase. Meanwhile, regulators are tightening oversight of automated decision making, children's data, health metrics, and cross-border data transfers. And litigation over online data collection by companies continues to expand under various statutes, including wiretapping and pen register claims under the California Invasion of Privacy Act (CIPA), and claims under the Video Privacy Protection Act (VPPA), resulting in diverging court rulings that send mixed signals to companies regarding privacy compliance.

This report examines the most significant developments shaping the privacy and AI landscape in 2025 and highlights practical steps businesses can take to navigate an increasingly complex, multi-jurisdictional legal landscape.

# Navigating the Shifting AI Landscape: What U.S. Businesses Need to Know in 2025

Artificial intelligence is no longer a wild west frontier technology—it's a regulated one. As AI systems become central to how companies operate, communicate, and compete, legal oversight is catching up. In 2025, AI governance is defined by divergence: a harmonized, risk-based regime in the EU; a fragmented, reactive framework in the U.S.; and rapid regulatory expansion at the state and global levels. Businesses deploying or developing AI must now navigate a multi-jurisdictional patchwork of laws that carry real compliance, litigation, and reputational consequences.

This article outlines the key regulatory developments, contrasts the EU and U.S. approaches, and offers concrete recommendations for U.S. companies operating AI systems.

**EU AI Act: Global Reach with Teeth**

The EU AI Act, which entered into force in August 2024, is the world's first comprehensive, binding legal framework for AI. It classifies systems by risk level—unacceptable, high, limited, and minimal—and imposes extensive obligations on high-risk and general-purpose AI (GPAI) models. High-risk AI systems must undergo pre-market conformity assessments, maintain technical documentation, and register in a public EU database. GPAI models face additional transparency, copyright, and cybersecurity obligations, particularly if they exceed scale thresholds (e.g., >10,000 EU business users).

The Act's extraterritorial reach means U.S. companies offering AI products or services in the EU—or whose outputs affect EU residents—must comply. Notably, failure to implement the EU's "voluntary" GPAI Code of Practice could shift the burden of proof in enforcement actions.

**Timeline to Watch:** The law becomes enforceable starting August 2026, with GPAI obligations phasing in from 2025.

**The U.S. Approach: Fragmentation, Tension, and State-Level Acceleration**

**Executive Orders & Federal Initiatives**

U.S. federal law remains sectoral and piecemeal. President Biden's 2023 Executive Order on "Safe, Secure, and Trustworthy AI" established guiding principles, including fairness, transparency, and privacy protections, and tasked agencies with issuing AI-specific standards. However, this was rescinded in 2025 by the Trump administration's new EO prioritizing deregulation and "American leadership in AI," creating a sharp policy pivot and regulatory uncertainty. In parallel, the administration also unveiled a draft *AI Action Plan*, emphasizing voluntary industry standards and innovation incentives over binding rules. While still in flux, this initiative further underscores the unsettled political climate around federal AI policy.

While bills like the AI Accountability Act and the SAFE Innovation Framework have been proposed, no comprehensive federal AI law has passed. Instead, federal agencies like the FTC, EEOC, and CFPB continue to regulate AI through existing consumer protection and civil rights laws—often through enforcement actions rather than formal rulemaking.

**State Spotlight: Colorado, California, and Others Lead the Way**

Absent a comprehensive federal law, states have moved decisively. The list below highlights a representative sample of enacted state AI statutes as of July 2025; dozens of additional bills are pending and advancing every legislative cycle:

**Arizona**

- **HB 2175** – requires health-insurer medical directors

to personally review any claim denial or prior-authorization decision that relied on AI, exercising independent medical judgment (in force on June 30, 2026).

California
- **AB 1008** – expands the CCPA definition of "personal information" to cover data handled or output by AI.
- **AB 1836** – bars commercial use of digital replicas of deceased performers without estate consent.
- **AB 2013** – requires AI developers to post detailed training-data documentation.
- **AB 2885** – creates a uniform statutory definition of "artificial intelligence" (effective January 1, 2025).
- **AB 3030** – mandates clear gen-AI disclaimers in patient communications from health-care entities (effective January 1, 2025).
- **SB 1001 "BOT" Act** – online bots that try to sell or influence votes must self-identify.
- **SB 942 AI Transparency Act** – platforms with >1M monthly users must label AI-generated content and provide a public detection tool.

Colorado
- **SB 24-205 – Colorado AI Act** – first comprehensive U.S. framework for "high-risk" AI; imposes reasonable-care, impact-assessment, and notice duties on developers and deployers (effective 2026).
- **SB 21-169** – bans unfair discrimination by insurers through algorithms or predictive models.
- **HB 23-1147** – requires deep-fake disclaimers in election communications.
- **Colorado Privacy Act** – consumers may opt out of AI "profiling" that produces legal or similarly significant effects; DPIAs required for such processing.

New York
- **New York City – Local Law 144** – employers using automated employment-decision tools must obtain an annual independent bias audit and post a summary.

Tennessee
- **HB 1181 – Tennessee Information Protection Act** (2024) – statewide privacy law; impact assessments required for AI profiling posing significant risks.
- **"ELVIS Act"** (2024) – makes voice mimicry by AI without permission a Class A misdemeanor and grants a civil cause of action.

Texas
- **Texas Data Privacy and Security Act** – lets Texans opt out of AI profiling that has significant effects and compels risk assessments for such uses.

Utah
- **SB 149 "AI Policy Act" (amended by SB 226)** – requires disclosure when consumers interact with generative-AI chat or voice systems and sets professional-licensing guardrails.
- **HB 452 – "Artificial Intelligence Applications Relating to Mental Health"** – regulates the use of mental health chatbots that employ artificial intelligence (AI) technology.

Expect additional Colorado-style comprehensive AI frameworks to surface in 2025-26 as states continue to fill the federal gap.

Global Developments & Cross-Border Tensions

Beyond the EU and U.S., countries like Brazil, China, Canada, and the U.K. are advancing AI governance through a mix of regulation and voluntary standards. Notably:

- China mandates registration and labeling of AI-generated content.
- Brazil is poised to pass a GDPR- and EU AI Act-style law.
- The U.K. continues to favor a principles-based, regulator-led approach but may pivot toward binding regulation.

U.S.-EU divergence has triggered geopolitical friction. The EU's upcoming GPAI Code of Practice is a flashpoint, with U.S. officials warning it could disproportionately burden American firms. Meanwhile, the U.S. may reconsider participation in multilateral frameworks like the Council of Europe's AI Treaty.

## A Compliance Playbook for 2025

AI legal exposure increasingly mirrors privacy law: patchwork rules, aggressive enforcement, and high reputational stakes. To mitigate risk, companies should:

- **Inventory AI Systems:** Identify all AI tools in use—especially those making or influencing decisions in high-risk sectors (HR, healthcare, finance, etc.).
- **Conduct Risk Assessments:** For GPAI or high-risk tools, assess training data, bias exposure, and explainability. Use frameworks like NIST's AI RMF or the EU's conformity checklist.
- **Build Cross-Functional Governance:** Legal, compliance, technical, and product teams must coordinate. Assign AI risk ownership and create change triggers for reclassification (e.g., changes in use or scale).
- **Monitor State and Federal Law Developments**.
- **Plan for EU Market Entry:** Determine whether EU-facing AI systems require local representation, registration, or conformity assessment under the AI Act.
- **Audit Communications:** Avoid AI-washing. Public statements about capabilities, safety, or human oversight must match internal documentation and performance.

The message from global regulators is clear: innovation is welcome, but governance is non-negotiable. Whether operating domestically or globally, businesses must prepare for AI compliance to become a core legal discipline, akin to privacy or cybersecurity.

For legal teams and compliance leaders, now is the time to move from principles to programs—and to see governance as a competitive advantage, not just a regulatory burden.

# U.S. State Privacy Laws: 2025 Status Update

By the end of 2025, eight new states will have enacted comprehensive privacy laws: Delaware, Iowa, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Tennessee. With twenty states expected to have such laws effective by year's end and more than a dozen additional states actively considering similar legislation for 2026 and beyond, businesses must continue to navigate an increasingly complex and fragmented regulatory landscape. While all state privacy laws share common core principles such as transparency in notice, data minimization, and opt-out rights for certain data usage, other aspects such as applicability thresholds, consumer rights, and enforcement mechanisms vary significantly across jurisdictions, all in the absence of a unifying federal privacy framework.

**General Principles of State Privacy Laws**

Certain baseline privacy principles remain consistent across all states. Businesses operating in any jurisdiction should provide clear notices to consumers about how their data is collected, used, and disclosed, and should limit the use of data collected to specific, disclosed purposes. Businesses should ensure they are collecting only the data necessary for legitimate business purposes and using it solely for the purposes stated in clear and conspicuous privacy notices.

**Consumer Rights**

Most states grant consumers a core set of rights that typically include the ability to access, delete, and correct personal data; request copies of their data (data portability); and opt out of targeted advertising, the sale of personal data, and certain types of profiling. However, there are notable exceptions. Iowa's law does not provide consumers with the right to correct inaccurate data or to opt out of processing for targeted advertising and profiling, limiting individual control compared to other states. In contrast, Minnesota extends consumer protections by allowing individuals to understand the basis of profiling decisions, access the data used, and pursue alternative outcomes. Minnesota also grants a transparency right (similar to Oregon's and Delaware's) allowing consumers to request a list of third parties that have received their data. Maryland takes a more limited approach, allowing consumers to request a list of categories of third parties to whom their data has been disclosed.

**Opt-In Preferences and Data Protection Impact Assessments**

All state privacy laws require businesses to honor opt-out requests, and some require respect for universal opt-out preference signals through mechanisms such as Global Privacy Control (GPC), which allow consumers to communicate their preferences regarding the sale of personal data and targeted advertising across all websites without needing to opt out individually. Amidst enforcement attention on this topic from California regulators, new laws in Delaware, Nebraska, New Hampshire, and New Jersey require recognition of such signals, with Maryland and Minnesota set to align by the end of the year.

Many new state laws also require businesses to conduct data protection impact assessments ("DPIAs") and/or internal or external audits when engaging in "high-risk" processing. This typically includes activities such as selling or sharing data for targeted advertising, profiling, or processing sensitive personal information.

**Sensitive Information**

All state privacy laws, including those taking effect in 2025, impose heightened restrictions on the collection and processing of sensitive information, and several expand what qualifies as "sensitive." New categories include national origin (Delaware, Maryland, New Jersey), transgender or non-binary status (Delaware, Maryland, New Jersey), biometric data (Maryland, Tennessee), and certain financial account information

(New Jersey). Maryland's law is particularly stringent, with a broad definition of "consumer health data" that includes information related to gender-affirming treatment and reproductive or sexual health care, and it prohibits processing or sharing sensitive information unless strictly necessary for a consumer-requested service even with consent. Additionally, new state laws in Delaware, Maryland, Nebraska, New Hampshire, New Jersey, and Tennessee follow several already enacted state laws in requiring businesses to conduct DPIAs when processing sensitive data or engaging in other high-risk activities.

**Applicability Thresholds of State Privacy Laws**

Determining which state privacy laws apply to your business requires careful analysis. While California, Tennessee, and Utah use revenue-based thresholds (e.g., $25 million) either alone or in combination with other factors, most states rely on volume-based criteria, typically applying to businesses that process the personal data of 100,000+ residents or derive a certain portion of revenue from selling data.

Several states have lower or broader thresholds:

- **Montana:** Applies to businesses collecting personal information of 50,000 consumers, or 25,000 if 25%+ of revenue comes from data sales.
- **Maryland, New Hampshire, Delaware, Rhode Island (2026):** Thresholds begin at 35,000 residents, with Delaware and Rhode Island also using a 20% revenue qualifier.
- **Texas and Nebraska:** Among the broadest, apply to nearly any business that is not a "small business" under SBA definitions, with no numerical data thresholds.
- **Florida:** Applies only to large for-profit companies with $1 billion+ in global revenue and certain tech-related operations.

Adding to the complexity, California uniquely includes employee, contractor, job applicant, and business-to-business transaction data under its CPRA, while most other states limit "consumer" to individuals acting in a personal or household context.

As a result, businesses must be aware of their data collection and processing activities in each state with a privacy law, and must analyze those activities against the requirements of each applicable state law.

**Enforcement of State Privacy Laws**

Like most state privacy laws, the 2025 statutes do not authorize any private rights of action (California remains the exception for certain data breaches involving sensitive personal information). Enforcement authority generally lies with each state's Attorney General (or, in California, its newly created Privacy Protection Agency), who are expected to take a more active role in investigating compliance and responding to consumer complaints, especially involving sensitive personal data. Most of the new laws also include cure periods, giving businesses an opportunity to correct violations before enforcement proceeds. Notably, New Jersey's law grants rulemaking authority to the Director of the Division of Consumer Affairs, signaling that additional implementing regulations may follow, similar to frameworks in California and Colorado.

A unique provision in Tennessee's law introduces an affirmative defense to enforcement actions – the first of its kind among U.S. privacy statutes. Businesses may invoke this defense by demonstrating that they maintain a written privacy program that "reasonably conforms" with the National Institute of Standards and Technology (NIST) privacy framework or a comparable standard. This incentivizes the adoption of widely recognized best practices and supports a more proactive approach to privacy compliance.

**Takeaways for Businesses**

With twenty comprehensive privacy laws expected to be effective by the end of 2025 and many more under consideration, privacy compliance is a national business imperative. Although discussions around a federal privacy law continue, no such law has yet materialized. As in the past, companies cannot rely on potential federal intervention to alleviate the burden of multi-jurisdictional compliance.

It is essential for all businesses to consistently map their data collection, use and disclosure, update privacy policies and notices, implement consumer

rights requests mechanisms, honor opt-out and limitation requests, and continue to monitor evolving requirements and implement scalable, principle-based privacy programs that can adapt to a shifting—and ever-increasing—patchwork of obligations.

See the U.S. State Privacy Laws - Applicability Thresholds chart on page 26 for more details.

# Developments in Digital Privacy Litigation in 2024-2025: CIPA, VPPA, and California's SB 690

In the wake of an explosion in digital privacy litigation, courts and legislatures are redrawing some of the boundaries of what qualifies as unlawful data collection under decades-old statutes. Claims brought under California's Invasion of Privacy Act (CIPA) and the federal Video Privacy Protection Act (VPPA) have tested how far traditional wiretap and video privacy laws can stretch to cover modern tracking technologies like pixels, session replay tools, and embedded analytics software. As these suits proliferate, courts are being asked to decide whether routine digital tracking amounts to interception, surveillance, or unauthorized disclosure of personal information.

Recent developments reflect both the tightening and expansion of privacy liability. In California, courts remain split on whether modern tracking tools qualify as "pen registers" or violate CIPA's wiretap provisions, while a pending bill—SB 690—aims to sharply curtail such claims going forward. At the federal level, VPPA decisions have moved in divergent directions, with a growing Circuit split on what makes someone a "consumer" and what counts as "personally identifiable information." Together, these trends show a legal landscape in flux, shaped as much by statutory interpretation as by shifting expectations around digital privacy and surveillance.

**California CIPA Developments**

Recent decisions illustrate the divergent paths CIPA claims are taking in California and beyond. While some courts continue to reject CIPA suits targeting ordinary website tracking, others are permitting such claims to proceed—especially where plaintiffs allege unauthorized use of third-party tracking software or more invasive data collection. The result is a patchwork of outcomes that often turn on the specific tracking technologies and legal theories alleged.

**What Counts as a "Pen Register" or "Trap and Trace Device" Under § 638.51?**

Courts are divided on whether modern web-tracking tools fall within the scope of California Penal Code § 638.51, which prohibits unauthorized use of devices that capture dialing or routing information, but not communication content.

In some recent decisions, courts have permitted claims to proceed where plaintiffs plausibly alleged that tools like TikTok scripts or IP trackers functioned like pen registers or trap-and-trace devices:

- *Lillian Jurdi v. MSC Cruises (USA) LLC*, No. 24STCV14098 (Cal. Super. Ct. Sept. 17, 2024): TikTok tracking scripts that collected geographic information, referral tracking, and URAL tracking could qualify as such devices.
- *Shah v. Fandom, Inc.*, No. 3:23-cv-4883 (N.D. Cal. Oct. 21, 2024): IP tracking that relayed user location data supported a pen register claim, as did the fact that users could not reasonably expect that trackers would be installed on websites and transmit their IP addresses every time they visited.
- *Heiting v. IHOP Restaurants, LLC,* No. 24STCV14453 (Cal. Super. Ct. Oct. 28, 2024): TikTok scripts plausibly captured incoming user data that identified that user like a trap-and-trace device.
- *Lesh v. CNN*, No. 1:23-cv-7374 (S.D.N.Y. Feb. 20, 2025): Court noted *in dicta* that IP tracking might fit the definition, particularly where it collected location-related data associated with user communications.

Others have rejected such claims, holding that § 638.51 targets telephone surveillance and doesn't extend to routine online tracking:

- *Sanchez v. Cars.com*, 2025 WL 487194 (Cal. Super. Ct. Jan. 27, 2025): The pen register statute does not extend to internet communications.
- *Rodriguez v. Plivo,* 2024 WL 5184413 (Cal. Super. Ct. Oct. 2, 2024): Basic location data revealed by

an IP address is not sensitive enough to sustain a pen register claim.
- *Palacios v. Fandom,* No. 24STCV11264 (Cal. Super. Ct. Sept. 24, 2024): IP addresses are not outgoing communications, as required to plausibly allege violation of the pen register statute.
- *Aviles v. LiveRamp*, No. 23STCV28190 (Cal. Super. Ct. Jan. 28, 2025): Tracking beacon collected only IP addresses and device information so did not qualify as a pen register.

**Session Replay and "Reading" in Transit under § 631(a)**

Courts assessing CIPA § 631(a) claims based on session replay tools have focused on whether the software *"reads"* communications *during transmission*. The statute prohibits unauthorized interception, but not all data capture qualifies—liability generally requires real-time comprehension or decoding.

Several decisions highlight this distinction between passive recording and active interception:

- *Heerde v. Learfield Communications LLC,* No. 2:23-cv-5258 (C.D. Cal. July 19, 2024): Court allowed the § 631(a) claim to proceed past the pleading stage where plaintiffs alleged that search terms were transmitted in real time to third parties, constituting interception in transit.
- *Torres v. Prudential Financial, Inc*., 2025 WL 1135088 (N.D. Cal. Apr. 17, 2025): Court granted summary judgment for defendants. The session replay software recorded keystrokes and mouse movements for later viewing but did not "read" the data as it was being transmitted. The absence of real-time decoding or interpretation defeated the CIPA claim.
- *Williams v. DDR Media, LLC,* 757 F. Supp. 3d 989 (N.D. Cal. 2024): After discovery, the court found that the tracking software hashed inputs and did not retain or analyze their contents. Because it neither read nor attempted to understand the meaning of the communications during transmission, no liability under § 631(a) attached and summary judgment was granted for the third-party vendor and defendant who partnered with it.

**Privacy Expectations in IP Addresses and Standing**

Defendants continue to win dismissal where courts find no reasonable expectation of privacy in IP addresses or where plaintiffs fail to allege a concrete injury.

- *Gabrielli v. Insider Inc.,* No. 1:23-cv-7433 (S.D.N.Y. Feb. 18, 2025): Dismissed for lack of standing; IP tracking alone didn't show harm or privacy invasion.
- *Zhizhi Xu v. Reuters News & Media,* No. 1:23-cv-7425 (S.D.N.Y. Feb. 13, 2025): Standing denied where plaintiff didn't allege that IP tracking resulted in targeting or other harm.
- *Heiting v. FKA Distributing Co.*, No. 3:23-cv-5329 (N.D. Cal. Feb. 3, 2025): No standing where plaintiff failed to specify frequency of visits, data shared, or whether the tracking led to any de-anonymization or harm.
- *Casillas v. Transitions Optical Inc.,* No. 23STCV30742 (Cal. Super. Ct. Apr. 23, 2024): Dismissed for lack of allegations about how plaintiff interacted with the site or what data was collected.
- *Ingrao v. AddShoppers, Inc.*, 2024 WL 4892514 (E.D. Pa. Nov. 25, 2024): Held that email addresses and general internet activity are not sensitive enough to support standing under CIPA or similar statutes.

**The Ninth Circuit Weighs in with Three Decisions**

Amidst these varying district court cases, the Ninth Circuit weighed in on three CIPA cases, affirming dismissal of CIPA claims in two cases, but reversing dismissal in a third case. These decisions will likely be used by both plaintiffs and defendants going forward in bringing and defending against CIPA claims:

- *Thomas v. Papa John's*, 2025 WL 1704437 (9th Cir. June 18, 2025): Affirmed dismissal of CIPA claims based on session replay code because plaintiff alleged that Papa John's *directly* violated § 631(a) by eavesdropping, as opposed to aiding and abetting eavesdropping by a third party. The panel held that a party to a conversation cannot be liable for eavesdropping on its own conversation.
- *Mikulsky v. Bloomingdale's,* 2025 WL 1718225 (9th Cir. June 20, 2025): Reversed dismissal of CIPA claims based on session reply code on defendant's

website, holding that the complaint alleged sufficient facts to allege that defendant aided or conspired with third-party session reply providers to capture the "contents" of plaintiff's communications on defendant's website (including names, addresses, credit card information, and product selections), and not merely "record" information (such as mouse clicks or movements) regarding the characteristics of those communications.
- *Guiterrez v. Converse*, 2005 WL1895315 (9th Cir. July 9, 2025): Affirmed dismissal of CIPA claims based on chat feature provided on Converse website by Salesforce because plaintiff provided no evidence that her chats were read by Salesforce, despite evidence that Salesforce could read those chats. Note concurrence by Judge Bybee questioning whether CIPA was intended to cover internet communications at all: "If the California legislature wanted to apply § 631(a) to the internet, it could do so by amending that provision or adding to CIPA's statutory scheme . . . California has failed to update § 631(a) to account for advances in technology since 1967. It is not our job to do it for them." *Id*. at *3.

**The VPPA Circuit Split in the Digital Age**

**Background**

The VPPA prohibits video service providers from knowingly disclosing a consumer's personally identifiable information (PII) related to video viewing without consent. Congress enacted the statute in 1988 after Judge Robert Bork's video rental history was disclosed during his Supreme Court confirmation process. Although the titles—such as Hitchcock thrillers and family films—were unremarkable, the episode sparked public concern over the ease with which viewing habits could be exposed. Following what became known as the "Bork Tapes" episode, Congress passed the VPPA to protect disclosure of consumers' video viewing information without their consent.

**The Second Circuit Expands, Then Narrows, the VPPA**

In *Salazar v. National Basketball Association*, 118 F.4th 533 (2d Cir. 2024), the plaintiff subscribed to the NBA's email newsletter and later viewed videos on NBA.com while logged into Facebook. He alleged that the NBA used Meta's tracking pixel to share his personal information and viewing history and Facebook ID with Meta for targeted advertising. The Second Circuit held that the email newsletter constituted a "good or service" under the VPPA even though it was non-video content. This holding significantly expanded the definition of a "subscriber" under the statute and led to a surge in VPPA claims.

More recently, however, in *Solomon v. Flipps Media, Inc.*, 2025 WL 1234567 (2d Cir. May 1, 2025), the Second Circuit held that sending a Facebook user's ID and a URL containing a video title to Meta does not trigger VPPA liability. Applying an "ordinary person" standard, the court ruled that this data combination does not constitute PII because it doesn't, on its own, reveal an individual's viewing history without additional tools or expertise. *Solomon* is a major victory for defendants and is expected to significantly curb pixel-based VPPA claims in the Second Circuit. The decision aligns the Second Circuit with the Third and Ninth Circuits, reinforcing a narrower interpretation of the statute.

**The Sixth Circuit's VPPA Limitation: *Salazar v. Paramount Global***

In *Salazar v. Paramount Global*, 133 F.4th 642 (6th Cir. 2025), the Sixth Circuit rejected a VPPA claim based on Meta Pixel use, narrowing the definition of "consumer" under the statute. The plaintiff alleged that 247Sports.com disclosed his video viewing history to Facebook while he was logged into his account and subscribed to the site's newsletter. The court held that unauthorized disclosure of viewing history to Facebook constituted a concrete injury, analogizing it to common-law privacy harms. However, it concluded that Salazar did not have a "consumer" relationship with the defendant, as required under the VPPA—Salazar's newsletter subscription didn't qualify as a subscription to goods or services in the nature of audiovisual materials.

**The Seventh Circuit's Expansion of VPPA Viability: *Gardner v. Me-TV National Limited Partnership***

In *Gardner v. Me-TV National Limited Partnership,* 132 F.4th 1022 (7th Cir. 2025), the Seventh Circuit expanded the scope of VPPA liability by holding that plaintiffs who created free MeTV accounts to access personalized video features qualified as "subscribers" under the statute. The plaintiffs alleged that MeTV embedded Meta's tracking pixel in its videos,

transmitting their viewing history and personal data to Facebook for targeted advertising. The court found that exchanging email addresses and zip codes for personalized video access made the plaintiffs "subscribers," emphasizing that "data can be worth more than money" in the digital economy. It adopted a broad reading of "consumer," holding that the VPPA covers anyone who subscribes to any service from a video tape service provider, regardless of whether the subscription is tied directly to video content. The court rejected MeTV's argument that the plaintiffs merely subscribed to an "information service," explaining that the statute focuses on who provides the subscription—not the specific type of content accessed. Gardner marks a significant expansion of VPPA exposure, particularly for ad-supported platforms that collect user data in exchange for personalized video features.

**Takeaways**

Together, *Solomon v. Flipps Media*, *Salazar v. Paramount Global*, and *Gardner v. Me-TV* illustrate the deepening Circuit split over how broadly the VPPA applies in the context of modern digital tracking. The Circuits have taken different positions on who qualifies as a "consumer" and what constitutes "personally identifiable information" traceable to a person. These cases underscore the uncertainty that remains around the VPPA's reach in the age of ad-supported streaming and pixel-based analytics, with the permissibility of such claims now hinging heavily on jurisdiction.

**SB 690: California's Legislative Response to CIPA Abuse**

Amidst the wave of CIPA litigation, the California legislature has introduced a bill to curb increasingly abusive litigation practices over website data collection that have surged over the past few years.

**What the Bill Does**

SB 690 amends CIPA to exempt from liability the use of recording or tracking technologies that serve a "commercial business purpose." The exemption applies to Penal Code Sections 631, 632, 637.2, and 638.51, provisions that have been the focus of extensive litigation and have generated significant uncertainty for businesses attempting to navigate compliance. The bill aims to clarify the permissible use of common and now universally used web technologies that assist with analytics, advertising, and personalization of digital experiences. If passed, the bill will rein in what many see as an increasingly unmanageable and unpredictable wiretapping litigation landscape.

**Who's Affected**

- **Defendants Favored**: Website operators, analytics providers, and ad tech firms gain protection from CIPA suits arising out of standard business activities.
- **Plaintiffs' Bar Constrained**: Routine lawsuits over standard tracking implementations lose statutory footing.
- **Businesses See Reduced Exposure and Litigation Cost**: Currently, CIPA permits $5,000 per statutory violation, and litigation costs on top of that create hefty financial repercussions for CIPA violations.

**Status and Outlook**

SB 690 passed the California Senate unanimously and also found strong support in the Assembly. As amended, the bill applies prospectively only—it will not affect pending cases filed before the effective date. However, the Assembly voted to advance the bill as a two-year bill, meaning that it can carry over into the 2026 legislative session and will likely delay enactment of the bill. This may prompt a further surge of CIPA filings over the next few months as plaintiffs race to file before the new limitations take effect.

**Conclusion**

As courts and lawmakers confront the realities of digital tracking and data analytics, the legal contours of privacy litigation are rapidly evolving. The mixed rulings under CIPA reveal a judiciary still grappling with how to apply legacy statutes to modern technologies, while the VPPA decisions reflect growing disagreement over the statute's scope in a data-driven economy. At the same time, SB 690 signals a legislative push to restore predictability and limit liability for businesses engaging in routine online practices. For companies operating in the digital space, this moment represents both risk and opportunity: a chance to reassess compliance strategies as privacy law realigns, and a need to stay alert as courts and legislatures continue to reshape the rules of engagement.

# CPPA Enforcement Actions: Key Lessons from Honda, Todd Snyder, and Healthline

The California Privacy Protection Agency (CPPA) is now in its second year with full enforcement powers and has begun to exercise its authority under the California Consumer Privacy Act (CCPA) in significant ways in 2025. With the creation of the CPPA and its recent assumption of enforcement authority, a new chapter of privacy rights enforcement has begun. Two recent enforcement actions against American Honda Motor Co. and menswear retailer Todd Snyder Inc. offer the most valuable insights to date into the CPPA's priorities and expectations. They also highlight operational privacy gaps of which companies of all sizes and in all industries should take note and work to comply with. And, California's Attorney General has reminded everyone that it is not to be forgotten in privacy enforcement, announcing the highest CCPA settlement to date in connection with a recent enforcement action involving health data.

**Case One: Honda – Verification, Cookies, and Contracts**

In March 2025, the CPPA announced its first enforcement order—a $632,500 administrative fine against American Honda Motor Co., one of the largest companies to face a formal enforcement action to date. The action stemmed from the CPPA's 2023 sweep of connected vehicle manufacturers, aimed at scrutinizing how automakers collect and share consumer data via in-vehicle systems and online platforms.

**Summary of Violations**

- **Oververification for Opt-Outs:** Honda required consumers submitting requests to opt out of the sale or sharing of their personal information—and requests to limit the use of sensitive personal information—to provide extensive personal details (including name, full address, phone number, and email). Unlike consumer requests for access, deletion and correction, which require identity verification, the CCPA rules prohibit such verification for opt out and limitation rights.
- **Confusing Agent Authorization:** The company also required consumers to confirm directly with Honda that they had authorized a third party to submit a request on their behalf, a practice explicitly disallowed by CCPA regulations for opt-out and limit-use requests.
- **Asymmetry in Cookie Management:** The CPPA found Honda's cookie consent banner violated design symmetry requirements. Consumers could "Accept All" cookies with a single click, but had to individually toggle off categories and confirm their choices to opt out—an unfair burden deemed to be a "dark pattern" under CCPA guidance.
- **Failure to Apply GPC to Known Users:** Honda did not extend Global Privacy Control-based opt outs to known users with accounts, limiting the scope of opt-out effectiveness.
- **Contractual Failures with Adtech Vendors:** Honda disclosed personal information to advertising technology partners without executing contracts that included required CCPA provisions, such as limitations on secondary use and data security commitments.

**Case Two: Todd Snyder – Infrastructure Failures and Excessive Data Collection**

In May 2025, the CPPA announced its second public enforcement order, this time against Todd Snyder Inc., a New York-based menswear retailer with several California locations. In settling with the CPPA, Todd Snyder agreed to pay a $345,178 fine and undertake numerous remedial steps. The case provides a useful contrast to Honda given that Todd Snyder is a smaller company facing many of the same privacy compliance challenges, but with different technical root causes.

**Summary of Violations**

- **Inaccessible Cookie Preferences:** For a period of 40 days in late 2023, a defect in the company's

cookie banner caused it to vanish before users could interact with it. As a result, consumers were effectively unable to opt out of tracking and behavioral advertising. This also meant that GPC signals were not honored during the outage.
- **Excessive Verification for AI Requests:** Todd Snyder required users to upload a photo ID for all privacy requests—including opt-outs and SPI limitation requests—despite the CCPA's clear prohibition on identity verification for these types of requests.
- **One-Size-Fits-All Request Portal:** Like Honda, Todd Snyder used a single webform for all consumer rights requests, failing to distinguish between verified and non-verified request types. This design flaw resulted in systematic overcollection of sensitive data.
- **Lack of Internal Oversight:** The CPPA emphasized that Todd Snyder failed to monitor its third-party privacy management tools and had no effective alerting system in place to catch or correct the cookie banner malfunction.

**Case Three: Healthline – Purpose Limitation and Privacy Expectations**

On July 1, 2025, the California Attorney General (AG) announced the largest settlement to date under the CCPA: a $1.55 million fine against Healthline Media LLC, a health and wellness website publisher. Unlike the CPPA-led actions against Honda and Todd Snyder, this enforcement was brought by the AG's office and underscores the ongoing parallel enforcement powers shared between the two agencies.

The case against Healthline marked the first CCPA enforcement action focused on health-related data, highlighting how regulators are applying the law's provisions to sensitive data practices even where traditional health privacy laws like HIPAA may not apply.

**Summary of Violations**

- **Failure to Honor Opt-Out Requests:** Healthline allegedly sold or shared consumers' personal information even after receiving opt outs, including Global Privacy Control (GPC) signals. Investigators found that third-party advertising cookies continued to collect and transmit information after consumers attempted to opt out.
- **Noncompliant Vendor Contracts:** The company shared personal data with advertising partners without including CCPA-mandated contractual provisions, such as purpose limitations and requirements for equivalent privacy protections by the recipient.
- **Purpose Limitation Violation:** This action is notable for including the CCPA's "purpose limitation" requirement—one of the first enforcements to do so. The AG alleged that Healthline's disclosure of article titles relating to medical conditions (e.g., Crohn's disease) to third parties for advertising purposes went beyond the purposes reasonably expected by consumers. This was true even if such sharing was technically disclosed in the privacy policy.
- **Deceptive Practices:** Healthline offered a cookie banner that appeared to allow users to disable advertising cookies but did not effectively do so, a practice characterized as deceptive under California's Unfair Competition Law (UCL).

**Enforcement Themes: Key Areas of CCPA Noncompliance**

The enforcement actions against Honda, Todd Snyder, and Healthline reveal a consistent set of compliance failures—and signal where California regulators are focusing their scrutiny.

- **Oververification**: Honda and Todd Snyder unlawfully required consumers to verify their identity for opt-out and SPI limitation requests. Todd Snyder even demanded photo IDs for all requests, violating the CCPA's data minimization principle.
- **Poor UX and Dark Patterns**: Honda's cookie interface made opting out harder than opting in, while Healthline's banner failed to function at all. The takeaway: design choices that confuse or burden users undermine valid consent and can lead to enforcement.
- **Technical Failures**: Todd Snyder's broken cookie banner and Healthline's ineffective opt-out tools show that nonfunctional systems—even due to vendor error—are the business's responsibility.
- **Ignoring GPC Signals**: All three companies failed to properly process Global Privacy Control (GPC)

signals. CCPA requires honoring GPC not only at the browser level, but across known user profiles.
- **Missing Vendor Contracts**: Honda and Healthline disclosed personal data to ad tech vendors without the required contracts limiting use, a recurring violation with high enforcement risk.
- **Purpose Limitation:** Healthline broke new ground by triggering enforcement under the CCPA's purpose limitation rule. Sharing article titles that suggest medical conditions for ad targeting went beyond what a reasonable consumer would expect—even if disclosed. The AG's action here probes into the subjective expectations of consumers, suggesting that even disclosed practices can be unlawful if they feel inherently invasive or unexpected. It also requires businesses to think hard about seemingly innocuous data like an article title that can become sensitive when tied to consumer identity.

**Final Thoughts: Functional Privacy, Not Just Formalities**

California regulators have made clear that privacy rights must be real, accessible, and aligned with consumer expectations. Enforcement is no longer just about having a policy—it's about making privacy work in practice. From broken cookie banners to overbroad data sharing, businesses subject to the CCPA should be proactively and carefully evaluating their practices and making necessary improvements.

# California Finalizes CCPA Regulations on Automated Decision-Making Technology, Risk Assessments, and Cybersecurity Audits

In July 2025, the California Privacy Protection Agency (CPPA) adopted final regulations governing automated decision-making technology (ADMT), privacy risk assessments, and cybersecurity audits under the California Consumer Privacy Act (CCPA). The final vote by the CPPA Board took place on July 24, following over a year of drafting and public comment.

The regulations now await approval by California's Office of Administrative Law (OAL). If the agency files them by the August 2025 deadline, they may become operative as early as December 1, 2025. Otherwise, the effective date will default to January 1, 2026. Businesses should not mistake this recalibration for retreat. The rules establish a practical but enforceable compliance regime—particularly for companies leveraging algorithmic tools, engaging in high-risk processing, or navigating overlapping state and global privacy frameworks.

**Recalibrating the Definition and Scope of ADMT**

The CPPA's final rules significantly narrow the scope of ADMT obligations to cases where technology "replaces or substantially replaces human decision making," removing explicit references to artificial intelligence and behavioral advertising use cases. This is a meaningful departure from the earlier, more expansive draft, which included tools that merely "facilitated" decisions or referenced artificial intelligence more broadly.

Under the revised rules, businesses are only subject to ADMT obligations when the technology is used to make "significant decisions," defined as those affecting financial services, employment, housing, education, or healthcare, or when they engage in certain types of profiling or train models for such use cases. Many previously covered scenarios, such as first-party advertising or public observation, have been removed entirely from the rule's opt-out and notice requirements.

Additionally, businesses no longer need to issue standalone "pre-use" notices. Instead, the revised rules allow them to integrate ADMT disclosures into existing notices at collection, easing administrative overhead while preserving transparency obligations.

**Narrowing Consumer Rights and Expanding Business Flexibility**

In line with its refined scope, the CPPA has pared back many of the consumer rights included in the original ADMT draft. Opt-out rights no longer apply to workplace or education profiling, public surveillance, or ADMT training activities. Instead, the rules focus on scenarios where ADMT is used to make determinations about core life opportunities—such as being hired, admitted to a school, or approved for a loan.

For these remaining "significant decision" use cases, businesses must provide a mechanism for consumers to opt out, or, in some cases, provide an appeal process reviewed by a qualified human decision-maker. The rules also introduce specific safeguards for biometric profiling and emotion-recognition systems, including accuracy evaluations and nondiscrimination audits.

Importantly, the final version of the rules appears likely to retain access rights to ADMT outputs, logic summaries, and decision making factors—but businesses will not be required to disclose trade secrets or details that could compromise fraud or safety defenses.

**Cybersecurity Audits: Scaled by Revenue, Governed by Independence**

The CPPA has also finalized a more risk-based and scalable cybersecurity audit framework. Under the revised draft, businesses that (i) meet the data broker threshold or (ii) process personal information of 250,000 consumers (or sensitive data of 50,000 consumers) must conduct an annual cybersecurity audit starting between 2028 and 2030, depending on revenue tier.

Audits must follow recognized professional standards and be certified by an executive responsible for cybersecurity. Auditors may be internal or external, but must be structurally independent. Key updates include:

- Businesses are no longer required to justify omitted safeguards (e.g., zero-trust architecture) or assess controls deemed inapplicable.
- Reports now require detailed explanations of any security gaps, plus a remediation plan, and must be retained for five years.
- A certification of audit completion must be submitted annually to the CPPA, beginning April 1, 2028, for larger entities.
- Internal auditors may now report directly to senior management, rather than the board, so long as they remain structurally independent from the cybersecurity function.

This flexible structure is intended to support scalability across organizations while preserving the CPPA's ability to scrutinize audit content and governance rigor.

**Risk Assessments: From Intrusive to Interoperable**

In a move praised by industry stakeholders, the CPPA has also walked back some of the more onerous elements of its proposed risk assessment requirements. Most notably:

- Full submissions are no longer required. Instead, businesses must retain the assessment and file only a certification and brief summary of key facts with the CPPA starting in 2028.
- Risk assessments are now required before a business (1) sells or shares personal information, (2) processes sensitive personal information, (3) uses ADMT for a significant decision concerning a consumer, (4) uses automated processing to infer attributes about an educational or job applicant, student, employee, or independent contractor, (5) uses automated processing to infer attributes based on a person's presence in a sensitive location, such as a medical facility, shelter, or place of worship, or (6) trains ADMT for any of those uses.
- Assessments must address detailed elements (purpose, types of personal information, specific processing operations, safeguards, stakeholder contributors, approver identity, and risks/benefits) and be approved by the business decision maker responsible for that activity. They must be reviewed at least every three years, or within 45 days of a material change to the processing activity. Starting April 1, 2028, businesses must annually report to the CPPA the number of risk assessments conducted, the types of processing activities and personal information involved, and submit an executive attestation, *under penalty of perjury,* that the assessments were completed.

**Strategic Implications and Compliance Planning**

These revised rules offer clearer paths for operationalization but shorten the lead time for implementation. Businesses that rely on ADMT or engage in high-volume or sensitive data processing should prioritize the following steps in the months ahead:

- **ADMT Mapping**: Inventory current assessments and incorporate the new CCPA triggers by year end.
- **Privacy Risk Framework Integration**: Evaluate whether existing DPIAs or AI assessments can be adapted to meet CCPA criteria. This is particularly critical for training use cases.
- **Audit Preparation**: Assign ownership for cybersecurity compliance and begin gap-mapping against the CPPA's control expectations, especially if audit certification deadlines fall in 2028 or 2029.
- **Executive Readiness**: Socialize the upcoming CPPA attestation requirement with your executive team and secure resources for the 2026-27 assessment cycle.

**Takeaways for Businesses**

The CPPA's latest rulemaking reflects a maturation of the CCPA framework, shifting the regulatory emphasis from consumer self-help to enterprise accountability. While the approved rules are more targeted and feasible than earlier drafts, they still demand robust documentation, governance, and strategic alignment across legal, privacy, and security teams.

The CPPA Board signaled it may revisit these rules as technology and market practices evolve, so anticipate further iterative adjustments.

# Updates to Children's Privacy Federal and State Laws

Over the past year, the Federal Trade Commission (FTC) has implemented significant updates to the Children's Online Privacy Protection Act (COPPA) Rule meant to strengthen key protections for children's privacy online. COPPA applies to children under the age of 13.

**Key Updates to COPPA Rule**

**Updated Requirements for Parents to Opt In to Third-Party Advertising**: Operators are now required to obtain separate verifiable parental consent before disclosing children's personal information to third parties for targeted advertising or other purposes. The Rule also expands on the methods on which parents can provide consent, which allows for authentication through (1) knowledge-based authentication through questions that no child under 13 could reasonably answer; (2) face-verification as compared to government-issued identification; or (3) text message to the parent coupled with additional steps for the parent to confirm their identity.

**Limitations Placed on Data Retention**: Operators are permitted to retain children's information for only as long as necessary to fulfill the specific purpose for which it is collected. Operators must establish, implement, and maintain a written data retention policy that specifies (1) the purpose for which the child's personal information was collected, (2) the specific business need for retaining such information, and (3) a timeline for deleting the information.

**Expanded Definition of "Personal Information":** The Rule updates the definition of personal information to now include biometric identifiers that are used for the automatic or semi-automatic recognition of an individual, including their fingerprints, handprints, retina patterns, genetic data, voice prints, and facial templates. This definition also includes government-issued identifiers, such as birth certificate, ID cards, and passport numbers. Notably, the Rule does not include "data derived from voice data, gait data, or facial data," which is language that was proposed in the 2024 NPRM.

**Enhanced Privacy Notice Requirements**: The Rule requires that the Operator's privacy notice include details about the specific internal operations for which persistent identifiers are collected, and how the operator ensures these identifiers are not used for any unauthorized purposes. Additionally, if audio files containing a child's voice are collected, the privacy notice must specify such collection is done solely to respond to a child's request and not for any other purpose, and that such collection will be immediately deleted.

**Written Information Security Program**: Operators must establish, implement, and maintain a written information security program that aligns with the sensitivity of the children's data they collect and their business's size and complexity. The program must include: (1) designated personnel to oversee it, (2) annual assessments of internal and external security risks to children's data, (3) implementation of safeguards to address those risks, (4) testing and monitoring of those safeguards, and (5) annual evaluation and updates to the security program.

**State Privacy Laws and Age Appropriate Design Code Laws**

While COPPA is meant to serve as a federal baseline for children's privacy, some states have adopted the Age Appropriate Design Code (AADC) legislation, which offers a more stringent set of protections. In the past year, several additional states have adopted their own versions, including Vermont and Nebraska. Other states that are considering AADC-style legislation include Connecticut, Illinois, Minnesota, New Mexico, and South Carolina.

While COPPA focuses on data collection and notice, AADC laws focus on the design aspects of a digital platform to ensure it is designed to protect the well-being and privacy of children, and it applies to all minors under the age of 18. AADC laws require platforms to design products with children's best interests in mind, using high privacy settings by default, minimizing data collection, and avoiding profiling or geolocation tracking unless strictly necessary. Operators must provide clear, age-appropriate explanations of how data is used and conduct risk assessments to identify and mitigate potential harms. The AADC laws also prohibit the use of dark patterns, which are manipulative design tactics that pressure minors into sharing data or making harmful choice. The AADC laws ensure platforms are built to support, not exploit, young users.

**Takeaways for Businesses**

Business collecting information of minors should be mindful in which state the minors live and what data is being collected so that they can comply with COPPA and AADC laws if applicable. Businesses should review and update their data collection, retention, and security policies to ensure compliance, and implement new practices as required by COPPA's latest update.

# Updates to U.S. Health-Data Privacy and Wearable Tech

This year marks a pivotal shift from the era of rapid, unregulated health-tech innovation to one of stringent governance. The proliferation of wearable devices, health applications and remote monitoring tools has led to an unprecedented expansion in legal oversight. New HIPAA regulations, state-level "sensitive health data" laws, and the FTC-broadened breach notification rules collectively underscore a unified message from regulators: safeguard health metrics across all platforms. Organizations handling any health-related data must now navigate an increasingly complex web of overlapping federal and state regulations to avoid significant legal repercussions.

**HIPAA Updates You Must Implement in 2025: Reproductive Health Privacy Rule**

In April 2024, the Department of Health and Human Services (HHS) issued a Final Rule under HIPAA aimed at strengthening privacy protections for reproductive health information. The rule, effective June 25, 2024, and with a compliance deadline of December 23, 2024, would have required covered entities to obtain a signed attestation before disclosing protected health information (PHI) related to lawful reproductive healthcare. It also mandated updates to Notices of Privacy Practices (NPPs) by February 16, 2026.

However, in a recent development, a federal district court in Texas vacated the rule on July 3, 2025, holding that HHS exceeded its statutory authority and violated the Administrative Procedure Act. The court's ruling halts enforcement of the reproductive health privacy rule nationwide unless overturned on appeal. As of now, the rule is not enforceable, and covered entities are not obligated to implement its provisions, although legal appeals may follow and some organizations may still voluntarily adopt its safeguards as a best practice.

For now, entities should monitor ongoing litigation and consider documenting their approach to reproductive-health disclosures in the event the rule is revived or replaced.

**HIPAA Security Rule Notice of Proposed Rulemaking**

On December 27, 2024, the Office for Civil Rights (OCR) at HHS issued an Notice of Proposed Rulemaking (NPRM) proposing significant amendments to the HIPAA Security Rule to bolster cybersecurity protections for electronic protected health information (ePHI). Key proposed changes include mandatory multi-factor authentication (MFA), encryption of ePHI both at rest and in transit, annual technical and non-technical evaluations, and a 24-hour breach notification requirement for business associates. No Final Rule on the matter has been issued.

**FTC Health Breach Notification Rule Now Applicable to Health Apps**

The FTC's amended Health Breach Notification Rule (HBNR), effective July 29, 2024, expands the scope of entities required to notify consumers and the FTC of breaches involving health information to apps and platforms not covered by HIPAA.

- Applies to fitness, fertility, mental health, and other apps tracking health data.
- Requires notification to consumers and the FTC within 60 days of breach discovery.
- Enforcement actions may include civil penalties.

**State Spotlight – Sensitive Health-Data Laws Beyond HIPAA**

Several states have enacted laws that treat biometric, wellness, geolocation, and inferred health data as sensitive, even when not covered by HIPAA:

**Washington – My Health My Data Act (MHMDA)**

- Effective March 31, 2024 (or June 30 for small businesses).

- Covers data "collected, derived, or inferred," including metrics from wearables.
- Requires opt-in consent and bans geofencing near reproductive health facilities (1,750 feet).

**California – Privacy Rights Act (CPRA)**

- Classifies wearable-derived metrics (e.g., heart rate, skin temperature, sleep) as "sensitive personal information."
- Grants consumers the right to opt out of sale or use and mandates data protection impact assessments (DPIAs).

**Texas – Data Privacy and Security Act (TDPSA)**

- Effective July 1, 2024.
- Covers biometric identifiers and physical health indicators.
- Entities must offer opt-out rights and adhere to purpose limitation and data minimization.

**Florida – Digital Bill of Rights (FDBR)**

- Effective July 1, 2024.
- Targets precise geolocation and biometric data, including data collected passively by connected devices.
- No cure period for violations—raising litigation risk for platform providers and developers.

**Intersections and Blind Spots**

The convergence of federal and state regulations creates complex compliance challenges, particularly for entities operating across multiple jurisdictions. For example, a wearable device used in a healthcare setting may be subject to HIPAA, while the same device used by a consumer falls under state laws like MHMDA or the CPRA. Employers providing wellness programs must navigate HIPAA, the Americans with Disabilities Act (ADA), and state privacy laws, depending on the nature of the data collected and its use.

**Takeaways for Businesses**

To navigate the evolving regulatory landscape, businesses should:

- **Conduct Comprehensive Risk Analyses:** Evaluate data flows to identify where health-related data is collected, stored, and shared.
- **Update Policies and Notices:** Revise privacy policies and Notices of Privacy Practices to reflect new legal requirements.
- **Enhance Security Measures:** Implement MFA, encryption, and other security controls as proposed in the HIPAA Security Rule NPRM.
- **Review and Amend Contracts:** Ensure business associate agreements and vendor contracts include provisions for breach notification and data protection.
- **Train Staff:** Educate employees on new privacy obligations and procedures for handling health-related data.

While HIPAA remains a foundational framework for health data privacy, the expanding landscape of state laws and FTC regulations necessitates a more comprehensive approach to compliance. Organizations must proactively assess their data practices, update security measures, and ensure transparency with consumers to navigate the complexities of health data privacy in 2025 and beyond.

# EU-U.S. Data Transfers in 2025

Cross-border data transfers between the EU and U.S. remain a legal and operational minefield. While the July 2023 adequacy decision ushered in the EU-U.S. Data Privacy Framework (DPF), recent developments have called its long-term stability into question. In parallel, both EU regulators and U.S. authorities have ramped up scrutiny of international data flows—ushering in a more complex, risk-sensitive compliance era for transatlantic businesses.

**The State of the Framework**

The DPF, designed to replace the invalidated Privacy Shield, allows certified U.S. companies to receive EU personal data without standard contractual clauses (SCCs) or transfer impact assessments (TIAs). But its legal foundation—U.S. Executive Order 14086—has come under renewed pressure following:

- Dismissals of key privacy oversight officials in the U.S.
- Structural changes to the Data Protection Review Court.
- Broad access authority granted to a new U.S. intelligence body—the Department of Government Efficiency (DOGE).

The European Commission has signaled support for maintaining the DPF but acknowledged that ongoing U.S. political developments could impact its sustainability. Legal challenges remain possible, and several supervisory authorities have advised against over-reliance.

**Enforcement is Real: The Uber Case**

In January 2025, the Dutch DPA fined Uber €290 million—the largest penalty issued by the regulator to date—for unlawful transfers of EU driver data to the U.S. without valid safeguards after discontinuing SCCs in 2021. Uber argued that GDPR's territorial scope negated the need for Chapter V safeguards. The DPA rejected this, reaffirming that data transfers must meet all GDPR conditions regardless of joint controllership claims.

The decision underscores that even global, well-resourced companies cannot afford gaps in transfer compliance.

**New U.S. Restrictions Create Reverse Pressure**

The compliance calculus is also shifting in the other direction. The U.S. Department of Justice's "Bulk Data Rule," effective April 2025, imposes strict restrictions on transfers of sensitive personal data from the U.S. to "countries of concern" (including China, Russia, and others). While aimed at national security, the rule applies to any U.S.-based entity—including those acting as processors for EU data—raising novel compliance challenges for onward transfers out of the U.S.

Implications include:

- Required audits and risk assessments.
- CISA-level cybersecurity obligations.
- Potential delays or restrictions for multinational vendor chains.

**Takeaways for Businesses**

To maintain compliant and resilient data transfer programs in this dynamic environment, organizations should:

- **Verify DPF Certifications**: Ensure U.S. recipients are currently certified and that the certification covers the specific data and processing purpose.
- **Retain SCCs and TIAs as a Backup**: Maintain robust documentation and fallback mechanisms in case the DPF is invalidated or suspended.
- **Monitor U.S. Bulk Data Rules**: Assess whether EU data processed in the U.S. is subject to onward transfer restrictions under the DOJ's new regime.
- **Conduct Ongoing Transfer Risk Reviews**: Include recent regulatory, legal, and political developments in third-country assessments.

- **Align Internal Definitions:** Ensure data transfer definitions match those used by EU authorities—including for remote access scenarios.
- **Anticipate Regulatory Questions:** Regulators may require granular evidence of safeguards, especially for transfers involving sensitive data (e.g., biometrics, employment, location).

While the DPF provides useful breathing room, it is not a bulletproof shield. EU-U.S. data flows remain structurally fragile, and organizations must layer compliance strategies—technical, contractual, and legal—to minimize exposure. Proactive alignment with evolving expectations on both sides of the Atlantic remains the best defense.

# U.S. State Privacy Laws - Applicability Thresholds

| State | Applicability Threshold |
|---|---|
| California | • Has gross annual revenue of $25 million or more; OR<br>• Controls or processes the personal data of 100,000 or more California residents; OR<br>• Derives 50% or more of its gross revenue from the sale of personal data. |
| Colorado | • Controls or processes the data of 100,000 or more Colorado residents; OR<br>• Derives any revenue from the sale of data for 25,000 or more Colorado residents. |
| Connecticut | • Controls or processes the data of 100,000 or more Connecticut residents; OR<br>• Derives 25% of its revenue from the sale of data for 25,000 or more Connecticut residents. |
| Delaware | • Controls or processes the personal data of not less than 35,000 Delaware residents; OR<br>• Controlled or processed the personal data of not less than 10,000 Delaware residents and derived more than 20% of their gross revenue from the sale of personal data. |
| Florida | • Has more than $1 billion in annual global revenue; AND satisfies at least one of the following:<br>  • Derives 50 percent of its global gross annual revenue from the sale of advertisements online; OR<br>  • Operates a consumer smart speaker and voice command service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; OR<br>  • Operates an app store or digital distribution platform with at least 250,000 different software applications for consumers to download and install. |
| Indiana | • Controls or processes personal data of at least 100,000 consumers (Indiana residents); OR<br>• Derives more than 50% of its revenue from selling the data of 25,000 consumers. |
| Iowa | • Controls or processes personal data of at least 100,000 consumers (Iowa residents); OR<br>• Derives more than 50% of its revenue from selling the data of 25,000 consumers. |
| Kentucky | • Controls or processes personal data of at least 100,000 Kentucky consumers; OR<br>• Controls or processes the personal data of 25,000 or more consumers and derives more than 50% of its gross revenue from the sale of personal data. |

| State | Applicability Threshold |
|---|---|
| Maryland | • Controls or processes personal data of at least 35,000 consumers, excluding data for the sole purpose of completing payment transactions; OR<br>• Controls or processes the data of at least 10,000 consumers and derives more than 20% of its gross revenue from the sale of personal data. |
| Minnesota | • Controls or processes the data of at least 100,000 consumers, excluding data for the sole purpose of completing payment transactions; OR<br>• Controls or processes the data of at least 25,000 consumers and derives more than 25% of its gross revenue from the sale of personal data. |
| Montana | • Controls or processes personal data of at least 50,000 consumers (Montana residents); OR<br>• Derives more than 25% of its revenue from selling the data of 25,000 consumers. |
| Nebraska | • Conducts business in Nebraska or produces a product or service consumed by Nebraska residents;<br>• Processes or engages in the sale of personal data; and<br>• Is not a small business as determined under the federal Small Business Act. |
| New Hampshire | • Controls or processes the personal data of not less than 35,000 unique consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; OR<br>• Controls or processes the personal data of not less than 10,000 unique consumers and derives more than 25% of its gross revenue from the sale of personal data. |
| New Jersey | • Controls or processes the personal data of 100,000 or more New Jersey consumers (excluding data used solely to complete a payment transaction); OR<br>• Controls or processes the personal data of 25,000 or more New Jersey consumers and derives revenue or receives a discount on the price of any good or service from the sale of data. |
| Oregon | • Controls or processes the personal data of not less than 100,000 Oregon residents; OR<br>• Controls or processes the personal data of not less than 25,000 residents and derives more than 25% of its gross revenue from the sale of personal data. |
| Rhode Island | • Controls or processes the personal data of 35,000 or more Rhode Island consumers (excluding data used solely to complete a payment transaction); OR<br>• Controls or processes the personal data of 10,000 or more consumers and derives more than 20% of its gross revenue from the sale of personal data. |
| Tennessee | • For-profit business with annual revenue of at least $25 million that controls or processes personal data of at least 175,000 Tennessee residents; OR<br>• Derives more than 50% of its revenue from selling the data of 25,000 consumers. |

| State | Applicability Threshold |
|---|---|
| Texas | • Conducts business in Texas or produces a product or service consumed by Texas residents and is not a "small business." |
| Utah | • Has more than $25 million in annual revenue and meets one or more of the following criteria:<br>  • Controls or processes the data of 100,000 or more Utah residents; and<br>  • Derives 50% or more of its revenue from the sale of data for more than 25,000 Utah residents. |
| Virginia | • Controls or processes the data of 100,000 or more Virginia residents; OR<br>• Derives 50% or more of its revenue from the sale of data for more than 25,000 Virginia residents. |

# Contact

If your company needs assistance with any privacy issues, the Coblentz Data Privacy and Cybersecurity attorneys can help. Please contact a member of the team below for further information or assistance.

## Authors


### Scott C. Hall

**Head of Data Privacy and Cybersecurity Group Partner**
San Francisco

**Contact**
415.772.5798
shall@coblentzlaw.com



### Mari S. Clifford

**Associate**
San Francisco

**Contact**
415.268.0504
mclifford@coblentzlaw.com



### Leeza Arbatman

**Associate**
San Francisco

**Contact**
415.293.6449
larbatman@coblentzlaw.com

## Katherine Gianelli

**Associate**
San Francisco

**Contact**
415.268.0594
kgianelli@coblentzlaw.com

## Saachi S. Gorinstein

**Associate**
San Francisco

**Contact**
415.268.0515
sgorinstein@coblentzlaw.com

## Hunter H. Moss

**Associate**
San Francisco

**Contact**
415.268.0595
hmoss@coblentzlaw.com

**Coblentz Patch Duffy & Bass LLP**
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com