Summary of 2025 State AG Privacy Enforcement Actions

Rebecca S. Engrav, Partner, Perkins Coie LLP
Aaron Haberman, Counsel, Perkins Coie LLP
November 7, 2025

Below, we summarize privacy enforcement actions (lawsuits or settlements) brought by state attorneys general in 2025 in California, Connecticut, Florida, Michigan, New York, Texas, and multistate. Then, we conclude with a few thoughts on trends for the future.

A. California

Sling TV, LLC

On October 30, 2025, the California Attorney General's office announced a $530,000 settlement with Sling TV, LLC, regarding alleged violations of the California Consumer Privacy Act (CCPA) and California's Unfair Competition Law. The complaint primarily concerns Sling's process for consumers to opt out of the sale or share of their personal information. According to the California AG, Sling used a combined cookie preferences and CCPA opt-out that was not enough to actually opt out of the sale of personal information; to fully opt out, consumers needed to find an embedded link in a webform and then click through confirmation steps. The AG also alleged that Sling (1) required consumers to provide their name, address, email, and phone number even if they were already logged in, and (2) did not provide a way to opt out through the Sling TV app, which the majority of consumers use to access Sling's services, and instead directed them to use a different device go to visit a URL that led to the inadequate cookie preferences setting. The complaint alleges these practices violated the CCPA's requirements to provide an easy to use opt-out method, provide an opt-out method in the manner in which the business primarily interacts with customers, provide easy to read and understandable disclosures and communications to consumers, and not require a consumer to provide additional information beyond what is necessary to exercise an opt-out.

The complaint also alleges that Sling further violated the CCPA by selling or sharing personal information and engaging in cross-context behavioral advertising with actual knowledge that consumers were under 16 without obtaining the required authorization. Specifically, the complaint alleges that Sling included channels and programming directed to children, had account and demographic information indicating the presence of individuals under 16 within subscriber households, and created audience segments based on children's age ranges—but did

not obtain consumer or parental authorization and did not turn off the collection, sale, and sharing of personal information when parental controls were turned on or children were likely to be watching.

As part of the settlement, Sling TV paid a $530,000 civil penalty and is subject to injunctive relief that includes a prohibition on directing consumers to Sling's cookie preferences page to exercise CCPA opt-out rights or requiring logged-in customers to fill out a webform to exercise the opt-out rights. Sling is also required to provide an opt-out mechanism within its Sling TV app, and to allow users to create kids' profiles for which the sale or sharing of personal information and cross-context behavioral advertising using personal information are turned off by default.

Todd Snyder

On May 6, 2025, the CPPA announced a $345,000 administrative fine against Todd Snyder for CCPA violations relating to consumer opt-out and data requests. The CPPA alleged that Todd Snyder: (1) imposed identity verification requirements for requests to opt out of the sale/share of personal information, which the CCPA prohibits; (2) required consumers to provide more information than necessary to submit privacy requests, even for requests for which companies can require verification (such as requests to delete or correct information); and (3) failed to properly oversee its privacy portal, operated by a third-party privacy compliance tool, leading to a misconfigured consent banner and a 40-day period during which consumers were unable to submit opt-out requests or send opt-out preference signals.

The order includes injunctive relief requiring Todd Snyder to (1) implement opt-out preference signals for known consumers and comply with CCPA requirements regarding opt-out preference signals; (2) stop requiring consumers to verify opt-out requests or provide more information than necessary for processing privacy requests; (3) identify and appropriately process disclosures of personal information that constitute a "sale" or "sharing" under the CCPA; (4) monitor and ensure the effectiveness of its opt-out request mechanisms; and (5) maintain appropriate contract management processes with third parties receiving personal information.

Honda

In a settlement announced in March, the CPPA imposed a $632,500 administrative fine on Honda, also relating in part to consumer sale/share opt-out requests. The CPPA alleged that Honda violated the CCPA by (1) imposing verification requirements for opt-out requests; (2) requiring consumers to provide more personal information than necessary to submit verifiable privacy requests; (3) required consumers to confirm opt-out requests submitted by their authorized agents; (4) used a cookie management tool that failed to meet CCPA's choice symmetry requirements by requiring consumers to toggle several settings and confirm their choices for opt-out requests while allowing a one-click opt-in; and (5) lacking required terms to protect consumers' privacy in contracts with parties with which Honda shared personal information.

The injunctive provisions in the Honda order include requirements to (1) implement a simpler process for consumers to assert their privacy rights; (2) consult with a UX designer to evaluate the company's methods for submitting privacy requests; (3) train employees regarding CCPA requirements; and (4) modify the company's contract management process to ensure that all required contractual terms are in place with third party recipients of data.

Healthline

In July, the California Attorney General's office settled with Healthline over alleged violations of the CCPA and California's Unfair Competition Law relating to Healthline's sale/share practices. According to the complaint, Healthline alleged that Healthline failed to comply with opt-out requests, continuing to provide personal information to over a dozen third parties involved in advertising even after receiving opt-out requests. The California AG also alleged that Healthline violated the CCPA's purpose limitation principle by sharing with advertising partners the titles of articles consumers read, which could be used to infer a current medical diagnosis. The purpose limitation principle provides that businesses may use personal information only for "the purposes for which [it] was collected" or "for another disclosed purpose that is compatible with the context in which [it] was collected." Civ. Code, § 1798.100, subd. (c); *see also* Cal. Code Reg., tit. 11, § 7002(b). The complaint also alleged that Healthline lacked CCPA-mandated terms in its contracts with parties with which it shared personal information.

Under the settlement, Healthline paid a $1.55 million civil penalty, the largest CCPA settlement to date, and agreed to injunctive terms requiring compliance with the CCPA. Healthline (1) is prohibited from selling/sharing personal information combined with information about articles read relating to medical diagnoses; (2) must notify consumers if it discloses sensitive personal information for advertising purposes and of their right to limit the use of their sensitive personal information; (3) must implement a CCPA compliance program and provide the AG annual assessments for a three-year period; and (4) must annually review its website and app to determine which parties it shares personal information with through tracking technologies and provide the AG a report on this, also for a three-year period.

California Data Broker Cases

Following an investigate sweep, the CPPA brought four lawsuits against data brokers for noncompliance with California's Delete Act, which requires data brokers to pay an annual fee and register in the CPPA's Data Broker Registry, with penalties for noncompliance of up to $200 per day plus the cost of registration and the CPPA's investigation and enforcement costs. In January, the CPPA settled with Connecticut-based Key Marketing Advantage, LLC for failing to register and pay an annual fee as required by the Delete Act. As part of the settlement, Key Marketing paid a $55,800 fine as well as the CPPA Enforcement Division's attorney fees and costs resulting from any future non-compliance.

In February, the CPPA settled with Background Alert, Inc., a California-based data broker, for failing to register and pay an annual fee as required by the Delete Act. According to the CPPA,

Background Alert created and sold consumer profiles based on billions of public records and drew inferences from those records to identify people who could be associated with searched-for individuals. The settlement required Background Alert to shut down operations through 2028.

In May, the CPPA ordered Jerico Pictures, Inc., d/b/a National Public Data, a Florida-based data broker, to pay a $46,000 fine for failing to register and pay an annual fee as required by the Delete Act. The CPPA stated that National Public Data registered as a data broker 230 days late, only after being contacted regarding noncompliance, and failed to challenge the CPPA Enforcement Division's administrative action seeking to fine the company for the Delete Act violations.

In July, the CPPA announced a settlement with Accurate Append over allegations that the company failed to register by the January 31, 2024, deadline for conducting business as a data broker in 2023, and registered only after being contacted by the CPPA. The stipulated order requires Accurate Append to pay a $55,400 fine, comply with the Delete Act's registration and disclosure requirements, and notify the CPPA if it ceases to operate as a data broker before the deadline to register.

B. Connecticut

TicketNetwork

On July 8, 2025, Connecticut Attorney General William Tong announced a $1.5 million settlement with TicketNetwork, following an investigation into the company's compliance with the Connecticut Data Privacy Act (CTDPA) and related consumer protection laws. The AG first sent TicketNetwork a CTDPA "cure notice" on November 9, 2023—four months after the law's effective date—highlighting deficiencies in the company's privacy notice. According to the AG, the notice was largely unreadable, did not address key data rights, and contained rights mechanisms that were misconfigured or inoperable. TicketNetwork was given 60 days to address these issues without penalty under the CTDPA's cure period, but allegedly failed to resolve the deficiencies well beyond the cure period. As part of the settlement, TicketNetwork will implement enhanced privacy and security measures, including stricter data protection protocols and improved transparency in ticket listings, and will be subject to ongoing compliance monitoring.

In a press release announcing the settlement, the AG's office stated that it had conducted four privacy notice sweeps, resulting in over two dozen cure notices issued to various entities to address privacy notice deficiencies, and that TicketNetwork was the only entity that repeatedly represented that it had resolved the identified issues when it had not, and failed to timely respond to follow-up correspondence from the AG's office.

C. Florida

Roku

Florida's lawsuit against Roku, filed in October, is based on practices by Roku with respect to children's personal information. Florida alleges Roku is violating the Florida Digital Bill of Rights (FDBR) by processing personal personal information with knowledge or willful disregard that users are under 18, and without providing the notice or obtaining the authorization or consent Florida requires for collection of minors' data. Florida also alleges Roku is violating the FDBR by processing and selling users' (not just minors') sensitive data without notice or consent, including by sharing users' geolocation data with the data broker Kochava. Finally, Florida alleges Roku is violating the FDBR by sharing deidentified data with third parties, including advertisers and data brokers, without taking reasonable measures to ensure the data cannot be associated with an individual or contractually obligating recipients of deidentified data to comply with Florida's prohibitions on reidentification. The suit is ongoing.

D. Michigan

Roku

Michigan also sued Roku, alleging violations primarily relating to Roku's collection and disclosure of children's personal information. The Michigan lawsuit, filed in April, alleges violations of COPPA (using states' power to enforce the law), the Michigan Consumer Protection Act. COPPA applies to services that are directed to children or that have actual knowledge that children use the service. The Michigan AG alleges Roku is directed to children in several ways, including because Roku has a Kids and Family section on The Roku Channel and promotes third-party apps on its streaming service that are targeted to children. The Michigan complaint alleges that Roku collects—and allows third party analytics companies and data brokers to collect—personal information such as locations, voice recordings, IP addresses, and persistent identifiers that track children's browsing histories on Roku and across the internet. According to the complaint, despite having services that are directed to children, Roku does not maintain child-specific profiles, settings, or notices, and does not alter these data collection practices based on whether a user is a child. The complaint thus alleges that Roku violates COPPA by knowingly collecting children's personal information without verifiable parental consent and without providing the required notice to parents, among other, related COPPA allegations. The Michigan complaint also alleges Roku violated (1) the Video Privacy Protection Act, 18 U.S.C. § 2710, by knowingly disclosing customers' video materials or services to third parties; (2) Michigan's Preservation of Personal Privacy Act, M.C.L. § 445.1711, by disclosing personal information showing customers as having purchased or rented particular videos; and (3) the Michigan Consumer Protection Act, M.C.L. § 445.901 et seq., for misrepresentations and omissions relating to the above data collect and disclosure practices. The suit is ongoing.

E. New York

National General/All State

On March 10, 2025, the New York Attorney General's office announced a lawsuit against National General and its owner, Allstate Insurance Company, regarding alleged security failures resulting in two data breaches. According to the AG, National General's insurance quoting websites by design displayed driver's license numbers in plain text, and in 2020, attackers exploited this to access the driver's license numbers of nearly 12,000 individuals, including more than 9,100 New Yorkers. The AG alleged National General failed to detect this for more than two months, failed to notify consumers or regulators, and left driver's numbers exposed on separate quoting websites. According to the AG, attackers then targeted the quoting system in a second, larger breach, compromising the personal information of an additional 187,000 consumers (including driver's license numbers of around 155,000 New York residents). The AG alleges that National General's security failures continued after Allstate acquired National General and took control of National General's data security function. In its complaint, the AG alleges violations of New York laws including the Stop Hacks and Improve Electronic Data Security (SHIELD) Act and New York's UDAP and false advertising statutes relating to the failure to notify consumers and New York agencies of the breach, failure to maintain reasonable security safeguards, and alleged misrepresentations regarding National General's data security practices. The matter is ongoing.

F. Texas

Allstate

In January, Texas sued All-State and its subsidiary, Arity, which claims to have the "world's largest driving behavior database." According to the Texas AG, Arity paid app developers to add Arity's software development kit (SDK) to their apps so that Arity could track driving data for more than 45 million consumers and create its driving behavior database. Allstate allegedly then used that behavior to inform car insurance premiums for consumers. The AG alleged Allstate violated the Texas Data Privacy and Security ActTDPSA by (1) failing to provide consumers notice about its processing of their sensitive data; (2) failing to provide consumers notice about sale of their sensitive data; (3) failing to obtain consumers' consent to process their sensitive data, as even if consumers consented to an app's collection of their sensitive data, they were not consenting to Arity's collection via the SDK; (4) failing to clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process; and (5) failing to provide consumers notice of how they can exercise their rights, including opt-out rights. The AG also alleged violation of Texas's Data Broker Law's registration requirement and violation of Texas's insurer-specific UDAP law for failing to verify consent to collect driving data, turning a blind eye to the probability that consumers did not consent, using the data for insurance underwriting, and marketing the data to insurers as driving behavior data. The case is ongoing.

G. Multistate

Illuminate Education, Inc. (California, New York, and Connecticut)

In November, the California, Connecticut, and New York AGs announced separate settlements totaling $5.1 million with Illuminate Education, Inc., an edtech company, over data breach between December 2021 and January 2022 that exposed millions of students' data, including medical information. According to the AGs, Illuminate left a former employee's credentials active years after the employee departed, and the hacker leveraged these credentials to create a new account and steal and delete student data over several days. The AGs alleged Illuminate failed to implement basic security measures, including by leaving former employee credentials active and failing to audits of credentials, failing to implement appropriate real-time monitoring and alerting for suspicious activity, lacking safeguards to protect backup databases, remind school districts to review student data held on their behalf for retention and deletion purposes. The AGs' other allegations include that Illuminate failed to notify regulators of the breach and made misleading representations regarding its data security practices. The case is the first action brought under Connecticut's Student Data Privacy Law; New York also alleged that Illuminate violated its education privacy laws that establish privacy and data security requirements for contractors who receive student data, Education Law § 2-d(5)(f); 8 NYCRR Part 121.9(a)(2), (a)(3), (a)(6), and (a)(7); and 8 NYCRR Part 121.10(a). As part of its settlements with the AGs, Illuminate must establish and maintain a comprehensive information security program.

H. Looking Ahead: Increased Enforcement and Collaboration Among States

The trend of increased enforcement is likely to continue next year, as states gain new enforcement powers and build privacy enforcement coalitions. The newly formed Consortium of Privacy Regulators—whose members include the CPPA and state AGs from California, Colorado, Connecticut, Delaware, Indiana, New Jersey, and Oregon—has the express goal of coordinating enforcement across states, taking advantage of similarities between their privacy laws. Three member states—California, Colorado, and Connecticut—recently launched a joint investigative sweep targeting businesses who do not appear to be processing requests to opt out of the sale of personal information submitted via the Global Privacy Control, as required by law.

Although smaller states show great interest in using their new enforcement abilities under new privacy-focused laws, California will likely remain the dominant privacy enforcer among the states, following a busy enforcement year for both the CPPA and the California DOJ. In recent remarks, Michael Macko, the CPPA's Deputy Director of Enforcement, characterized the agency as entering "a new era of privacy enforcement" and said it currently has "hundreds of open

investigations." As for the agency's enforcement priorities, in the near term, we expect to see continued focus on compliance with California's opt-out requirements. To that end, CPPA Executive Director Tom Kemp has said the agency is focused on launching its DROP (Delete Request and Opt-out Platform) in January, which would let consumers send a single request to all registered data brokers to require them to delete personal information.