RETROSPECTIVE

US POLICY

U.S. Privacy Enforcement in 2025

U.S. Legislation & Regulation

February 2026

Authored By: **Jordan Francis**, Senior Policy Counsel, U.S. Legislation
Daniel Hales, Policy Counsel, U.S. Legislation
Jameson Spivack, Deputy Director, Artificial Intelligence
Tatiana Rice, Senior Director, U.S. Legislation

FUTURE OF PRIVACY FORUM

Executive Summary

The U.S. privacy law landscape continues to mature as new laws go into effect, cure periods expire, and regulators interpret the law through enforcement actions and guidance. Nineteen U.S. states have enacted comprehensive consumer privacy laws. Sectoral laws have also proliferated, addressing topics such as biometric privacy, youth privacy and online safety, health and reproductive privacy, data brokers, financial privacy, artificial intelligence and automated decisionmaking, and more. State attorneys general and the Federal Trade Commission act as the country's de facto privacy regulators, regularly bringing enforcement actions under legal authorities both old and new. For privacy compliance programs, this steady stream of regulatory activity both clarifies existing responsibilities and raises new questions and obligations.

This Retrospective looks at state and federal U.S. privacy law enforcement in 2025 and identifies four key trends and insights:

1. **California and Texas Lead Growing Public Enforcement of Comprehensive Privacy Laws:** Comprehensive privacy laws may finally be moving from a period of legislative activity into a new era where enforcement is shaping the laws' meaning, as 2025 saw a significant increase in the number of public enforcement actions.
2. **States Demonstrate Increasing Concern for Kids' and Teens' Online Privacy and Safety:** As legislators continue to consider broad youth privacy and online safety legal frameworks, enforcers too are looking at how to protect the youth online. Bringing claims under existing state laws, including privacy and UDAP, regulators are paying close attention to opt-in consent requirements, protections for teenagers in addition to children under 13, and the online safety practices of social media and gaming services.
3. **U.S. Regulators Go Full Speed Ahead on Location and Driving Data Enforcement:** Building on recent enforcement actions concerning data brokerage and location privacy, federal and state enforcers have expanded their consumer protection enforcement strategy to focus also on first-party data collectors and the collection of "driving data."
4. **FTC Prioritizes Enforcement on Harms to Kids and Teens, and Deceptive AI Marketing, Under New Administration:** The FTC transitioned leadership in 2025, moving into a new era under Chair Andrew Ferguson that included a shift toward targeted enforcement activity focused on ensuring children's and teens' privacy and safety, and "promoting innovation" by addressing deceptive claims about the capabilities of AI-enabled products and services.

In conclusion, we note several practical takeaways that compliance teams can draw from these trends: obtaining required consent prior to processing sensitive data, including through oversight of vendors' consent practices, identification of known children, and awareness of laws with broader consent requirements; ensuring that consumer controls and rights mechanisms are operational; avoiding design choices that could mislead consumers; considering if and when to deploy age assurance technologies and how to do so in an effective and privacy-protective manner; and avoiding making deceptive claims about AI products.[1]

[1] The appendix in this resource contains a table of relevant case materials and a brief description of each.

Acknowledgements

The authors thank U.S. Policy Interns Rafal Fryc and Christian Seremetis for their contributions to this retrospective. This work builds on FPF's June 2024 report *Top Six Major Privacy Enforcement Trends: A U.S. Legislation Retrospective*.

Table of Contents

I. Walking the Walk: California and Texas Lead Growing Public Enforcement of Comprehensive Privacy Laws

In the 2024 version of this report, FPF noted a lack of public enforcement activity pursuant to state comprehensive privacy laws. Although attorneys general had long been bringing privacy lawsuits under existing legal authorities, such as UDAP, there had only been three public enforcement actions under the new wave of comprehensive privacy laws despite many of those laws having been in effect for months or years. That changed in 2025, however, as fifteen new enforcement actions were publicly announced, filed, or settled.[2] California and Texas led that charge and were joined by Utah, Florida, and Connecticut who all announced first lawsuits or settlements under their respective laws. **The significant increase in public enforcement actions signals that U.S. state comprehensive privacy laws are moving from the legislative chambers into a new enforcement era.**

California

The California Department of Justice (DOJ) and the California Privacy Protection Agency (CalPrivacy) concurrently enforce the California Consumer Privacy Act (CCPA). These enforcers announced six new CCPA settlements in 2025, double the number reached between 2022 and 2024. **The DOJ's settlements overwhelmingly focused on the selling/sharing of personal information and advertising practices.** Of note, the DOJ reached a $1.55M settlement with publisher Healthline Media. That action focused on collection and use of personal information in advertising. The DOJ alleged that Healthline failed to honor "do not sell or share" opt-outs (including GPC signals), did not have CCPA compliant contracts with third parties, and acted deceptively under the state's Unfair Competition Law by offering a cookie banner that purported to allow them to disable advertising cookies but did not do so in reality. Additionally, this was the first settlement to interpret the purpose limitation requirements in the CCPA regulations. Among the personal information Healthline allegedly shared with advertisers and data brokers were article titles which suggested that individual visitors were diagnosed with specific medical conditions (e.g., "Newly Diagnosed with HIV? Important Things to Know"). **The DOJ alleged that this conduct violated section 7002 of the CCPA regulations, which limits the collection and use of personal information to what is consistent with consumers' reasonable expectations.** To the DOJ, sharing such information that potentially reveals sensitive health-related information with third parties for targeted advertising would not be expected by a reasonable consumer.

In a settlement with SlingTV, the DOJ alleged that the company had insufficient and overly burdensome opt-out procedures. The conduct at issue included combining cookie preferences with the CCPA opt-out (despite disabling cookies being insufficient to opt-out of targeted advertising), requiring customers to locate an embedded link and use a multi-step confirmation process to complete an opt-out, requiring too much information from logged-in customers to exercise their opt-out, not providing opt-out methods within apps on connected devices, and failing to comply with heightened kids' and teens' protections (see Part II below). Similarly, in a

[2] This figure counts Texas's five lawsuits against connected tv manufacturers as those lawsuits constituted public cure notices.

later settlement with Jam City, the DOJ alleged that the company failed to obtain required opt-in consent before selling the personal information of adolescents aged 13 through 15 (see Part II below) and that the company failed to provide CCPA compliant opt-out mechanisms across many of its mobile applications.

CalPrivacy's settlements were more varied but tended to focus on the ease of exercising consumer rights. In CalPrivacy's first settlement under the CCPA, with connected vehicle manufacturer Honda, the agency focused on the user experience and asymmetrical privacy controls. The alleged conduct at issue included unnecessary verification to exercise certain rights, offering a non-symmetrical (1 click vs 2 click) opt-out banner, making it difficult to allow authorized agents to exercise rights, and sharing personal information with ad tech companies without necessary contracts in place. Notably, the settlement required the company to consult a user experience (UX) designer to evaluate its methods for submitting privacy requests. Similarly, in a settlement with clothing retailer Todd Snyder, the agency alleged that the company unnecessarily required verification to exercise opt-out rights, unnecessarily collected sensitive personal information for exercising verified consumer rights, and failed to monitor its third-party privacy management tool (resulting in 40-day delay in processing opt-out requests). The agency's third settlement, with lifestyle retailer Tractor Supply Company, alleged that the company failed to maintain a privacy policy that notified consumers of their rights, failed to notify job applicants of their privacy rights and how to exercise them, failed to provide consumers with an effective opt-out (sell/share) mechanism (including through opt-out preference signals), and disclosed personal information to other companies without entering into CCPA-required contracts.

Data Brokers and Delete Act in Focus: CalPrivacy enforces the Delete Act in addition to enforcing the CCPA. This law applies to a subset of businesses under the CCPA that are also data brokers—defined under the law as businesses that knowingly collect and sell to third parties the personal information of a consumer with whom the businesses do not have a direct relationship. Failure to register as a data broker remains a persistent enforcement focus for CalPrivacy. The agency announced a public investigative sweep of data broker registration compliance, launched a "Data Broker Enforcement Strike Force" in its enforcement division, and issued an enforcement advisory concerning data broker registration.

CalPrivacy reached four settlements under the Delete Act in 2025, most of which primarily dealt with businesses' failure to register with CalPrivacy as a data broker. One settlement involved a business that searches public records (e.g., births, arrests, marriages and divorces) and provides compiled reports on a searched-for individual. The reports also include inferred information, such as "people possibly associated with the searched-for individual" and "alarming patterns" in the individual's public records. That settlement re-affirms prior guidance from the Attorney General that inferences derived from publicly available information are personal information under the CCPA. In another settlement involving inferences, the agency clarified that businesses providing advertising and marketing services act as data brokers when they disclose consumers' personal information to third parties. In the agency's words, "[a] sale is a sale." The company in question derived insights about consumers (e.g., creating a "fitness" audience segment based on data indicating the consumer attends a health club),

enriched first-party data, aggregated third-party data, and offered precise targeting based on "geospatial intelligence" and demographics. This trend looks likely to continue, as the agency announced two additional settlements with data brokers concerning non-registration in January 2026.

Texas

Travelling east, Texas bolstered its claim as a leading privacy enforcer in 2025. No stranger to enforcing privacy rights under the Deceptive Trade Practices Act (DTPA) and the Capture or Use of Biometric Identifier Act (CUBI), Texas became the first state to file an active lawsuit (as opposed to an investigation or settlement) under a state comprehensive privacy law in January. As part of a broader trend concerning the collection and use of driving behavior data (see Part III below), Texas announced a lawsuit in January 2025 against insurer Allstate and the company's data broker subsidiaries (all going by some variation of "Arity"). The conduct at issue concerned the alleged collection and sale of sensitive consumer data without sufficient notice or consent under the Texas Data Privacy and Security Act (TDPSA). The companies were alleged to be collecting this sensitive data (specifically precise geolocation data) via a software development kit integrated into third-party apps and subsequently using that data for insurance purposes. Later in the year, the Attorney General announced lawsuits against five different tv manufacturers concerning the use of automated content recognition technology to capture and disclose consumers' viewing habits for use in targeted advertising. Although none of these complaints included claims under the TDPSA, each complaint included a footnote declaring that the allegations in the lawsuit serve as notice of TDPSA violations and failure to cure would see the complaint amended to add additional claims.

Utah

California and Texas may have been at the forefront of comprehensive privacy law enforcement in 2025, but they were not alone. Staying in the Southwest, Utah also filed a first lawsuit under the Utah Consumer Privacy Act (UCPA) in June. Youth privacy and online safety remains a top enforcement focus for regulators (see Part II below), and the focus of this lawsuit was social media platform Snapchat's design features that allegedly "addict children; harm their mental health and wellbeing; and facilitate illegal drug sales, sexual exploitation, sex trafficking, [and] the distribution of pornography." The alleged violations under the UCPA were (1) sharing personal data and conversation details with third parties in contradiction of the platform's privacy policy which claimed that the company does not share private communications with service providers, (2) failure to provide consumers with clear notice or ability to opt-out of sensitive data collection through the My AI feature, which allegedly collects geolocation data and biometric data, and (3) processing the personal data of known children without obtaining verifiable parental consent.

Florida

Traveling further east, Florida also brought a first lawsuit under the Florida Digital Bill of Rights (FDBR) in October. The AG alleges that Roku, a content platform for connected televisions, processed and sold sensitive data (e.g., precise geolocation data and children's personal data) without consent. Since its enactment, there has been much debate about whether the FDBR is a "comprehensive" consumer privacy law due to its narrow applicability thresholds—most of the law applies only to controllers who generate at least $1B in annual revenue and either (a) derive 50%+ of global annual revenue from the sale of advertisements online, (b) operate a consumer smart speaker and voice command component service with an integrated virtual assistant, or (c) operate an app store or a digital distribution platform offering at least 250K different software applications for download. In this case, the AG asserts that the company both derives 50%+ of its global annual revenue from the sale of advertisements online and operates a consumer smart speaker. **This case may be a warning for companies to reevaluate whether they are in scope of Florida's law.** Additionally, the law's prohibition on selling sensitive data without a consumer's consent applies more broadly to any for-profit entity who conducts business in Florida and collects personal data about consumers or is the entity on behalf of which such information is collected. This lawsuit serves as a reminder that those provisions can be enforced more broadly than the rest of the law.

Getting into the substance of the complaint, the AG faulted the company for failing to implement mechanisms to identify which users are children, which the AG argued was done to process and sell children's personal and sensitive data without getting parental consent by avoiding establishing "actual knowledge" under the law (see Part II below). The AG also alleged that the company sold users' sensitive data (including precise geolocation data) without consent and shared "deidentified" data without imposing legally-mandated contractual clauses preventing the recipient from reidentifying the consumers whose data are being disclosed.

Connecticut

Completing this cross-country tour, Connecticut also announced a first public settlement under the Connecticut Data Privacy Act. Although the text of the settlement is not accessible, the press release explains that TicketNetwork was fined $85K after failing to cure alleged violations following notice from the Office of the Attorney General. The allegations included having a deficient privacy notice (being "unreadable" and "missing key data rights"), having misconfigured and inoperable rights mechanisms, and inadequate responses to the cure notice (failing to respond in a timely manner and "repeatedly represent[ing] that they had resolved deficiencies when they had not done so").

* * *

Looking at this activity across these states, it is evident that 2025 saw a significant increase in public enforcement activity and that trend shows no sign of abating. The first weeks of 2026 saw CalPrivacy reach new data broker settlements and the Kentucky Attorney General filed a first lawsuit under the Kentucky Consumer Data Protection Act. As of January 2026, every state

comprehensive privacy law is in effect. Although amendments to certain laws may not have taken effect, and regulations are pending in multiple states, every law is currently enforceable to some degree. In many states, mandatory opportunities to cure have either sunsetted or been removed by amendments. U.S. state privacy law may finally be moving from legislative turmoil into an era dominated by enforcement of existing laws.

AG Reports Shed Light on Non-public Enforcement: Enforcers are also taking actions whose details are not fully public, such as sending letters of inquiry or issuing cure notices. Reports from attorneys general provide a behind-the-scenes look at enforcement in their respective states: Connecticut's second-annual report highlighted several enforcement topics, including privacy notices, facial recognition technology, marketing and advertising practices, palm recognition, connected vehicles, genetic data, and teens' data. In Oregon, the DOJ released an annual enforcement report covering the first year of enforcing the Oregon Consumer Privacy Act in addition to quarterly enforcement reports.

New Bipartisan Privacy Enforcement Consortium: Another portent of increased enforcement activity is the formation of a new, bi-partisan "Consortium of Privacy Regulators." Announced by CalPrivacy, the group includes the California Privacy Protection Agency and state Attorneys General from California, Colorado, Connecticut, Delaware, Indiana, New Hampshire, New Jersey, Minnesota, and Oregon. The consortium's purpose is to "share expertise and resources, as well as coordinate efforts to investigate potential violations of applicable laws." This information sharing could be highly impactful as regulators are able to leverage shared institutional capacity and technological expertise.

II. Major Focus on Protecting Minors Online: States Prioritize Youth Online Privacy and Safety Enforcement

Youth online privacy and safety has increasingly become a focal point of state legislators in the past few years, and, in 2025, protecting minors online appears to be a growing enforcement trend among state regulators as well. **Two broad themes emerged in the kinds of enforcements state regulators pursued to protect kids online: (1) Actions regarding minor data protection obligations, particularly respecting opt-ins and consent requirements; and, (2) Lawsuits targeting the online safety practices of social media and gaming services, typically brought under state consumer protection laws.**

Minor Data Collection, Opt-ins, and Consent

In 2025, a significant number of privacy enforcement actions involved a **company that allegedly knew minors used the service—demonstrated through child-specific content or experience offerings—and violated minor data protection obligations by collecting, processing, or sharing minor data without obtaining proper authorization or consent.**

For example, in the Sling TV settlement (see Part I), the California DOJ alleged that Sling TV knew children used the platform, citing its child-directed streaming content, household and consumer

data obtained from data brokers, and the availability of parental controls. Despite this knowledge, the DOJ alleged that Sling TV failed to limit data sharing, sale, or targeted advertising for "kids' profiles," did not implement age screening, and did not obtain the required opt-in consent from minors under 16 or from parents of children under 13. Just one month later, the California DOJ announced another settlement with Jam City, alleging similar violations of the CCPA's opt-in consent requirement for selling or sharing the personal data of consumers under 16 years of age. The DOJ alleged that Jam City knew children used its services because it implemented age gates and offered "child versions" of games that restricted data sharing or sale, but, for some of its apps, the company limited those protections to users under 13, leaving some users aged 13–15 subject to data sharing or sale without the required opt-in consent. Utah's lawsuit against Snap similarly alleged that the social media platform collected and disclosed the personal data of known children without verifiable parental consent.

In addition to California, both Michigan and Florida brought enforcement actions against Roku alleging comparable violations of data protection laws. In Michigan, the Attorney General brought a COPPA enforcement action against the media streaming provider, alleging that it collected and used children's data without parental consent despite knowing children used the service, as evidenced by child-directed content such as "Kids and Family" sections, "Popular Free Kids Movies and TV Shows" recommendations, and advertising aimed at children. Meanwhile, the Florida Attorney General brought an action against Roku under the Florida Digital Bill of Rights (FDBR), alleging that the company "decided not to implement industry-standard user profiles to identify which of its users are children," which the AG argued was done to process and sell children's personal data without obtaining parental consent by avoiding establishing "actual knowledge" under the law. Under FDBR, a controller "wilfully disregards" a consumer's age if it "should reasonably have been aroused to question whether a consumer was a child and thereafter failed to perform reasonable age verification." The complaint points to a number of age signals that could have prompted an inference that children were using the service, including content specifically designated for kids under the age of 9 and content labeled as "Made for Kids." The AG therefore alleges that the company processes the sensitive data of known children under 13 without performing age verification and without obtaining affirmative authorization or consent for such processing and selling of sensitive data.

Consumer Protection Lawsuits Addressing Child Safety

As the constitutionality of various emerging online safety frameworks continues to remain uncertain, like age appropriate design codes and social media safety laws, some state attorneys general are not waiting for new statutes to bring child online safety-related enforcement actions. **Instead, some AGs are turning to their state's preexisting consumer protection laws to bring claims against companies, broadly alleging a failure to implement sufficient safeguards despite representing the online services and features as safe for child and teen users.**

Amid states' heightened scrutiny of social media and online gaming companies for alleged failures to address clear risks of harm to young people—including child exploitation and grooming, access to harmful content, and certain "addictive" behaviors—Attorneys General in Florida (and here), Kentucky, Minnesota, Texas, and Utah filed lawsuits to advance online child safety agendas. Exercising their consumer protection authority in novel ways, these state AGs allege that companies engaged in unfair and deceptive practices by failing to implement

adequate safeguards for children online–such as age verification, adequate content moderation, or age appropriate experiences–and by misrepresenting that their services were safe for children even though they were aware of high risks of harm. Trends among AG arguments in these actions include:

- **Omitting known facts about the risks of harm to children:** AGs commonly allege that companies are in possession of unique and detailed internal information regarding the risks of harm posed by their services, products, features, and design practices, but they fail to disclose that necessary safety risk information to the public, constituting a deceptive trade practice.
- **Data practices:** Multiple lawsuits–including Florida, Kentucky, Minnesota, and Utah–address company data practices within claims alleging safety defects. Notably, some AGs broadly link design features that may expose young users to safety, privacy, or security harms to the collection and use of valuable consumer data, framing this as an alleged unfair and deceptive practice. For example, in Utah's complaint, the AG alleges that the platform drove young users to engage with a chatbot feature with known safety risks, which collected large volumes of sensitive data from children's chats and images to the company's benefit. The AG further alleges that the company deceptively failed to disclose these data practices in public-facing materials or privacy policies and misrepresented the feature as safe for use.
- **Misrepresentation:** AGs uniformly allege that named companies misrepresented platform or product safety to the public by claiming their service was safe for children and teens despite contrary internal information about known risks and a lack of adequate safeguards. For example, Minnesota's AG alleges that the company made public representations of platform safety, including through "Community Guidelines" and "'Newsroom posts,'" even though it allegedly knew about high risks of harm and "flawed" safety measures, including "policy grey areas . . . lack of adequate training, and under-resourced content moderation teams." Moreover, in Kentucky's complaint, the AG alleges that the company's public representations of platform safety are deceptive where it makes design choices and advertises safety measures that are purportedly unsafe or deficient, such as "ineffective chat filters" and "weak content moderation."
- **Calls for age verification:** Several attorneys general allege that a platform's lack of more robust age verification measures to identify children on the platform and implement adequate safeguards in user accounts is an intentional platform design choice contrasting against safety realities, constituting an unfair or deceptive trade practice.

Knowledge Inferred from Product Design and Content Offerings: Regulators are increasingly pointing to inclusion of child-directed content, kids and families sections or channels, advertising selections, parental controls, and age screenings within services as evidence that a company knew or should have known that children and teens used the company's service. Moreover, states utilizing an "actual knowledge or willful disregards" standard, such as Florida and California, are veering towards a constructive interpretation of this standard as regulators are increasingly evaluating whether companies should have questioned a users' age based on various signals and inferences, lowering the bar for enforcement from the stricter actual knowledge standard.

Accounting for Teens is a Compliance Imperative: Historically, child data protection obligations applied only to children under the age of 13. As states have enacted modern data protection laws in recent years, statutory age thresholds have expanded, affording new and heightened data protection obligations for teens in addition to children under 13. California's recent enforcement actions underscore a growing imperative for companies to pay attention to these expanding age thresholds and ensure compliance with special obligations to protect child ***and teen*** data, including providing opt-in consent for certain processing activities.

Shifting Tactics to Address Children's Online Safety: Recent enforcement activity suggests that consumer protection law may increasingly become a child safety enforcement tool, with AGs attempting to extend their deception and unfairness enforcement authority to online child safety contexts. If successful, states that establish child online safety enforcement through existing consumer protection laws may forgo pursuing emerging online safety proposals that offer similar protections but have been frequently subject to constitutional infirmity. Some state AGs are pursuing tech company accountability through consumer protection law with the same vigor they put into litigation against "big tobacco" conglomerates–adopting or extending strategies similar to those used against drug companies in addiction cases to hold technology companies accountable for alleged addictive behaviors, design defects, and related public health harms associated with certain platforms and services. Indeed, Minnesota's AG has expressly made such comparisons between the tobacco industry and social media services, claiming, "this stuff is digital nicotine."

III. Shifting Gears: U.S. Regulators Go Full Speed Ahead on Location and Driving Data Enforcement

Policymakers have long recognized that an individual's location is particularly sensitive personal data, and have sought to establish protections against its misuse. Until recently, that recognition largely translated into consumer protection enforcement, with State Attorneys General and the FTC targeting data brokers for alleged "unfair" and "deceptive" practices relating to precise location data. Recently, however, as cars have developed into so-called "computers on wheels," regulators have also begun scrutinizing how a range of entities—particularly data brokers, auto manufacturers, and insurance companies—collect, process, and sell both location *and* other data associated with vehicles. **As such, in 2025 regulators expanded their consumer protection**

enforcement strategy beyond third-party data brokers and location data, focusing also on first-party data collectors and "driving data."

Key examples of this shift are reflected in recent enforcement actions by state regulators in Texas and California, and then by the FTC. Following a compliance investigation into car manufacturers regarding their collection and sale of drivers' data, Texas AG Ken Paxton brought an enforcement action against General Motors (GM) in late 2024 and against Allstate Insurance (and its data-broker subsidiary Arity) in 2025, alleging that the companies engaged in unfair and deceptive trade practices by collecting and selling consumer's "driving data." In both cases, Paxton alleged that driving behavior and location data—collected through vehicle telematics systems (GM) or mobile app software development kits and third-party sources (Allstate)—was aggregated and sold to insurers in ways that influenced insurance decisions without consumers' knowledge or meaningful consent. The AG further alleged GM engaged in deceptive practices by making representations that such data would not be shared. The case against Allstate and Arity included claims under the Texas Data Privacy and Security Act (TDPSA), Texas's data broker registration law, and Texas's prohibition on unfair methods of competition and unfair or deceptive acts or practices in the business of insurance, illustrating the number of legal tools AGs have to bring privacy enforcement actions.

Federal and multistate enforcement soon followed. In January 2025, the FTC announced a proposed order settling allegations against GM and OnStar that closely matched AG Paxton's lawsuit (later finalized in 2026). Over the next few months, AGs in Arkansas, Indiana, and Nebraska all announced lawsuits against the company for similar alleged "deceptive" and "unfair" data practices. At the same time, comprehensive privacy laws provided regulators with additional tools to scrutinize location data practices. In Allstate, Texas AG Paxton also alleged five violations of the Texas Data Privacy and Security Act (TPDPA), while California AG Bonta initiated an investigative sweep of the location data industry under the CCPA, issuing letters to data brokers, advertising networks, and mobile app providers citing potential violations of consumers' rights to opt out of the sale or sharing of personal information and to limit the use of sensitive data, including precise geolocation.

These "driving data" lawsuits represent the latest evolution in a multiyear enforcement trend concerning location data. In their suits against Allstate and GM, regulators have:

- **Expanded their focus beyond location data to "driving data"**: The FTC and state AGs alleged that consumers' "driving" and "driving behavior" information—associated with a consumer's vehicle's elevation, speed, trip times, engine health, and hard acceleration and breaking—was collected and sold without consent. The FTC also alleged that Vehicle Identification Numbers (VINs) were used to link both driving data and geolocation data to specific drivers.
- **Expanded their focus beyond data brokers to first-party collectors**: Unlike the data broker lawsuits, regulators brought actions against parties that collected data directly from consumers. Moreover, AG Bonta's March 2025 investigative sweep of the location data industry targeted not just data brokers, but also mobile app providers and advertising networks that may be in violation of the CCPA, suggesting an expanding list of potential enforcement targets.

- **Focused on car manufacturers, particularly those that share data with third parties**: In their suits against GM, the FTC and state AGs all mention the company's partnership with the data brokers Verisk and LexisNexis. AG Paxton noted that Honda and Hyundai had entered similar agreements with Verisk, and in the *Allstate* case, AG Paxton mentioned that Allstate had purchased driving data from a number of other car manufacturers.
- **Brought claims under different laws for the same behavior**: In its case against GM, the FTC cited its Section 5 authority to enforce against "unfair" and "deceptive" trade practices, which was mirrored by the AGs' consumer protection law enforcement in Indiana and Nebraska (with Nebraska prohibiting "unconscionable" rather than "unfair" acts). Meanwhile, in their separate actions, the AGs in Texas and Arkansas alleged that GM's acts constituted violations merely of their states' prohibitions on "deceptive" trade practices. Relatedly, in his case against Allstate, AG Paxton brought counts under Texas' privacy law, data broker law, and insurance law, demonstrating how regulators may prosecute the same acts using multiple causes of action.

IV. Back to Brass Tacks: FTC Narrows Enforcement Focus on Kids and Teens and Deceptive AI Marketing under New Administration

Beyond the states, the FTC under Chair Andrew Ferguson has shifted toward enforcement actions addressing a narrower set of priorities, with avowed emphasis on children's and teens' privacy and safety and deceptive marketing and sales practices, particularly in the context of AI-enabled products. Many of these matters arose from conduct investigated under the prior administration, and their resolution during Chair Ferguson's tenure signals continuity in these areas, even as other initiatives have been deprioritized.

Kids' Privacy and Safety

As in the states, child privacy and safety took center stage in FTC priorities in 2025, with the FTC finalizing the COPPA rule in the Federal Register[3] (FPF redline here) and bringing or finalizing at least four enforcement actions related to kids' and teens' privacy or safety. In three cases, brought against Sendit (a mobile messaging app), Disney (related to Youtube), and Apitor (interactive robot toy with a companion app), the Commission alleged that the **companies violated the Children's Online Privacy Protection Rule (COPPA Rule) by knowingly collecting data from children under 13–whether known through user declarations or child-directed targeting–and failing to implement measures that allow for required parental notice and consent.**

Separately, in two of the cases, the FTC alleged that the business practices harming children *and teens* were deceptive trade practices in violation of Section 5 of the FTC Act. In Sendit, the Commission alleged that the company misrepresented the origin and authenticity of anonymous messages to induce users to purchase premium subscriptions. According to the FTC, some messages—marketed as peer-generated—were in fact fabricated and, in certain instances, adult-themed, exploiting children's and teens' susceptibility to online impersonation ("catfishing")

[3] *Note: FTC Chair Ferguson has also recently stated that he intends to re-open COPPA rulemaking.*

to drive paid upgrades. In Aylo (parent company of Pornhub), the Commission (in collaboration with the State of Utah) alleged that the company deceptively made public claims that there was "zero tolerance" for CSAM and non-consensual materials (NCM) despite hosting content (and encouraging users to upload content) that were tagged to suggest the content contains minors.

Deceptive AI Claims

Beyond kids' and teens' privacy and safety, the Commission also focused regulatory scrutiny on businesses that oversold the capabilities or traits of their AI products in violation of Section 5 of the FTC Act. The following types of performance-related claims related to AI products were purported by the Commission to be a deceptive trade practice:

- **Can Guarantee Profits:** In Air AI, the company claimed that their suite of AI-related business products, including conversational AI, would help businesses make tens of thousands of dollars. The Commission stated "at best, Defendants offer coaching that does not help consumers start or grow a business, glitchy software that does not perform as advertised, and licenses to resell the same. At worst, Defendants sell consumers a junk suite of services that do not exist or are not consistently available."
- **Accuracy:** In Workado and Intellivision, the companies claimed that their AI products maintained exceptional accuracy, with Workado claiming that their AI content detector could predict with 98.3% accuracy whether content was created by AI, and with Intellivision claiming that their facial recognition system exhibited "zero gender or racial bias." The Commission stated in both instances that the claimed metrics were not accurate, based on third-party testing sources such as NIST or publicly available external metrics.
- **Legal Tools:** In DoNotPay and accessiBe, the Commission challenged claims that AI tools could independently deliver legally compliant outcomes. DoNotPay allegedly marketed its product as a substitute for legal services despite not being a licensed law firm and while under investigation by the California Bar Association for unauthorized practice of law. In accessiBe, the Commission alleged that the company's claims of "automated accessibility compliance" were unsupported, citing expert assessments—including those from World Wide Web Consortium and Utah State University Institute for Disability Research Policy & Practice—that many websites labeled compliant were not.

The FTC Eyes Age Assurance and Chatbots: Recent FTC signals suggest potential future focus on age assurance and chatbots. As part of Disney's settlement with the FTC, the company must establish and implement a program to review whether videos posted to YouTube should be designated as "Made for Kids" **unless YouTube implements age assurance technologies** that can determine the age, age range, or age category of all users. The FTC's explicit reference to age assurance is worth noting, and tracks with the Commission's recent age assurance workshop, remarks and discussions at the June 2025 Workshop, and a blog posted the same day as the Disney settlement. In that post, the FTC writes that "Effective age assurance technologies that reliably identify users' ages can ease the burden on parents, allow kids to have an age-appropriate experience online, and protect kids from harmful content online."

In parallel, the Commission has signaled increased attention to child-directed AI products and chatbots. Beyond the enforcement action against Apitor, an interactive robot toy with a companion app, the Commission ordered seven other major companies to provide information on how they measure, test, and monitor the impact of consumer-facing AI-powered chatbots on children and teenagers.

Appendix: Case Materials

Jurisdiction	Target	Description	Link(s)
Arizona	Temu	Similar to lawsuits filed by Arkansas, Kentucky, and Nebraska, this lawsuit alleges that the Temu app harvests users' sensitive data without consent and uses technical measures to mask this activity.	Press Release
Arkansas	General Motors, OnStar	This lawsuit alleges that the companies improperly collected driving data, which was then sold to third parties and further sold to insurance companies to deny insurance coverage or increase rates.	Press Release
California (DOJ)	Healthline	$1.55 million settlement and injunctive terms. The AG alleged that the company failed to honor "do not sell or share" opt-outs, shared information with advertisers and data brokers (including article titles which suggested that individual visitors were diagnosed with specific medical conditions) in a manner that was inconsistent with consumers' reasonable expectations, failed to have CCPA compliant contracts with third parties, and acted deceptively by offering a cookie banner that purported to allow them to disable advertising cookies but did not do so in reality.	Press Release
California (DOJ)	SlingTV	$530K settlement and injunctive terms. The AG alleged that the company had insufficient and overly burdensome opt-out procedures, including requiring customers to locate and embedded link and use a multi-step confirmation process to complete an opt-out, requiring too much information from logged-in customers to exercise their opt-out, not providing opt-out methods within apps on connected devices, and not offering kids profiles to reduce targeted advertising to children or obtain "opt-in" consent for targeted advertising to consumers who were likely under 16.	Press Release
California (DOJ)	Jam City	$1.4 million and injunctive terms. The complaint alleges that Jam City violated the CCPA by failing to obtain the required opt-in consent before selling the personal data of adolescents aged 13 to 15. It also alleges that the company failed to provide CCPA compliant opt-out mechanisms across 21 of its mobile applications.	Press Release
California (CalPrivacy)	Key Marketing Advantage, LLC (KMA)	Failure to register as a data broker.	Press Release
California (CalPrivacy)	Jerico Pictures, Inc., d/b/a National Public Data	Failure to register as a data broker.	Press Release
California (CalPrivacy)	Background Alert, Inc.	Failure to register as a data broker.	Press Release
California (CalPrivacy)	Honda	$632.5K settlement and injunctive terms. The agency alleged that the company required unnecessary verification to exercise certain rights, offered a non-symmetrical (1 click vs 2 click) opt-out banner, made it difficult to allow authorized agents to exercise rights, and shared personal information with ad tech companies without	Press Release

Jurisdiction	Target	Description	Link(s)
		necessary contracts in place. As part of the settlement, the company is also required to consult a user experience (UX) designer to evaluate its methods for submitting privacy requests.	
California (CalPrivacy)	Todd Snyder	$345,178 fine and injunctive terms. The agency alleged that the company failed to monitor third party privacy management tool (resulting in 40-day delay in processing opt-out requests), unnecessarily required verification to exercise opt-out rights, and unnecessarily collected sensitive PI for exercising verified consumer rights.	Press Release
California (CalPrivacy)	Tractor Supply Company	$1,350,000 fine and injunctive terms. The agency alleged that the company failed to maintain a privacy policy that notified consumers of their rights, failed to notify job applicants of their privacy rights and how to exercise them, failed to provide consumers with an effective opt-out (sell/share) mechanism, and disclosed PI to other companies without entering into CCPA-required contracts.	Press Release
California (CalPrivacy)	ROR Partners	Failure to register as a data broker.	Press Release
Connecticut	TicketNetwork	While the AG's office did not release the official settlement, its press release stated that the company's notice “was largely unreadable, missing key data rights, and contained rights mechanisms that were misconfigured or inoperable.” The press release also alleged that the company repeatedly claimed it had resolved the issues but failed to do so.	Press Release
Federal Trade Commission	IntelliVision	The FTC alleged that the company made "false, misleading, or unsubstantiated claims that its AI-powered facial recognition software was free of gender or racial bias.	Press Release
Federal Trade Commission	Mobilewalla	The FTC alleged that the company sold sensitive location data without taking reasonable steps to verify consumers' consent. Sensitive location data included data identifying: health clinics, religious organizations, correctional facilities, labor union offices, LGBTQ+ related locations, political gatherings, and military installations.	Press Release
Federal Trade Commission	Cognosphere	The FTC alleged that the company did not obtain verifiable parents required by COPPA before collecting children’s personal information.	Press Release
Federal Trade Commission	DoNotPay	The FTC alleged that the company deceptively claimed to have made "the world's first robot lawyer."	Press Release
Federal Trade Commission	Avast	The FTC alleged that the company deceptively marketed to consumers that its product would block third party tracking, while it would sell their re-identifiable browsing data.	Press Release
Federal Trade Commission	Evolv Technologies	The FTC alleged that the company made misleading claims about its AI-powered security screening system.	Press Release
Federal Trade Commission	Empire Holdings Group	The FTC alleged that the company falsely claimed to help its users set up an "AI-powered Ecommerce Empire."	Press Release

Jurisdiction	Target	Description	Link(s)
Federal Trade Commission	GoDaddy	The FTC alleged that the company mislead consumers about its data security practices and compliance with the EU-US Privacy Shield Framework.	Press Release
Federal Trade Commission	Ascend Ecom	The FTC alleged that the company falsely claimed its users would generate an income through its AI-powered online storefronts.	Press Release
Federal Trade Commission	FBA Machine & Bratislav Rozenfeld	The FTC alleged that the company and owner deceptively guaranteed income through "AI powered" online storefronts and defrauded consumers.	Press Release
Federal Trade Commission	Air AI	The FTC alleged that the company made deceptive claims about its business growth tools, promising unrealistic returns and a "conversational AI" that can replace human customer service representatives.	Press Release
Federal Trade Commission	Workado	The FTC alleged that the company made misleading marketing claims when it offered an ineffectiveAI detection service for writing.	Press Release
Federal Trade Commission	Iconic Hearts Holdings	The FTC alleged that the company's anonymous messaging app, commonly used by children, collects data from children without obtaining verifiable parental consent and mislead users by sending messages from fake "people."	Press Release
Federal Trade Commission	Apitor	The FTC alleged that the company, a robot toy maker, enabled a third party in China to collect location information on children without parental consent, in violation of COPPA.	Press Release
Federal Trade Commission	Illuminate Education	The FTC alleged that the company, an educational technology provider, failed to implement an adequate data security program, allowing a hacker to access the personal data of more than 10 million students.	Press Release
Federal Trade Commission	Rytr	The FTC reopened and set aside the earlier Rytr order "in response to the Trump Administration's AI Action Plan."	Press Release
Federal Trade Commission	Disney	The FTC alleged that the company collected data from children watching child-marketed videos on YouTube without obtaining consent from parents.	Press Release
Federal Trade Commission	Kochava, Collective Data Solutions	The FTC alleged that Kochava obtained and sold consumers' precise geolocation—tied to a unique, persistent identifier and other personal data—to customers without consent. **[Note: This was not a 2025 enforcement action and is included here because of its relevance to Part III of this retrospective.]**	Case Summary
Federal Trade Commission	X-Mode Social, Outlogic	The FTC alleged that the company obtained and sold consumers' location data—tied to a unique, persistent identifier and timestamp, and in some cases other personal information—without consent. **[Note: This was not a 2025 enforcement action and is included here because of its relevance to Part III of this retrospective.]**	Press Release
Federal Trade Commission	InMarket Media	The FTC alleged that the company: collected consumers' location data through SDKs, which it embedded in its own proprietary apps,	Press Release

Jurisdiction	Target	Description	Link(s)
		for use in targeted advertising without providing proper notice or obtaining consent; failed to verify that third-party apps using its SDK had obtained informed consent to collect, use, and sell data for the purpose of targeted advertising; and retained this data longer than necessary for the stated purpose, increasing the risk of harm. **[Note: This was not a 2025 enforcement action and is included here because of its relevance to Part III of this retrospective.]**	
Federal Trade Commission	Gravy Analytics, Venntel	The FTC alleged that the company obtained and then sold consumers' precise geolocation data (tied to an individually identifiable Mobile Advertising ID (MAID)) without consent and failed to take reasonable steps to confirm consumers had consented to their data suppliers' collection, use, and sale of geolocation data.	Press Release
Federal Trade Commission	General Motors, OnStar	The FTC alleged that the company and its subsidiary collected consumers' precise geolocation and driving data and then sold this data to data analytics companies and consumer reporting agencies without providing notice or obtaining consent.	Press Release
Florida	Snap	The AG alleged that the company allowed minors under 16 to make accounts without parental consent and that the platform had addictive design elements, easily accessible harmful content, and deceptive practices in its marketing around platform safety.	Press Release
Florida	Roku	The AG alleged that the company decided not to implement "industry-standard user profiles to identify which of its users are children" and processed and sold children's personal data without consent. The complaint also alleges that the company is selling and sharing consumers' precise geolocation data with advertisers without consent and sharing "deidentified" data with the knowledge that recipients will reidentify consumers' identities.	Complaint
Florida	Roblox	The AG alleged that the company collected data from children under 13 without verified parental consent.	Complaint
Indiana	General Motors, OnStar	The AG alleged that the company used deceptive "dark patterns" during consumer onboarding to ensure they participated in a telematics system which collected consumers' location and driving data, failed to disclose to users that this data was sold to data brokers to create "risk profiles" regarding driving behavior, and then sold that data to insurance companies, all without consent.	Press Release
Kentucky	Temu	The AG alleged that the company's app surreptitiously collected extensive, sensitive personal data without notice or consent.	Complaint
Michigan	Roku	The AG alleged that the company collected the personal information of children and shared it with third parties without verifiable parental consent.	Complaint
Nebraska	Lorex Corporation	The AG alleged that the company deceptively failed to disclose that its security cameras were manufactured by a Chinese company responsible for both the hardware and software of the devices.	Complaint
Nebraska	Temu	The AG alleged that the company's e-commerce app collects	Press Release

Jurisdiction	Target	Description	Link(s)
		extensive, sensitive personal data without disclosure or consent in a way designed to evade app store privacy frameworks.	
Nebraska	General Motors, OnStar	The AG alleged that the company collected consumers' driving data through its telematics program, contracted with data brokers to create "telematics exchanges" that created risk scores for drivers based on this data without knowledge or consent, and this data was used to make decisions about consumers' insurance rates.	Press Release
Texas	Allstate, Arity	The AG alleged that the company and its subsidiary paid third party app developers to add its software development kits into their mobile apps, collected data about consumers' precise geolocation and the phone's speed, altitude, and longitude, then used the data for insurance purposes without consent.	Press Release
Texas	Google	$1.375 billion settlement. The settlement resolved three separate lawsuits filed in 2022 alleging that the company unlawfully collected and misused user data, including location information (filed 1/24/22), biometric identifiers (filed 10/20/22), and data obtained through the "Incognito" browsing mode (filed 5/19/22).	Press Release
Texas	Epic Systems	The AG alleged that the company's EHR "Foundation System" uses a deceptive, automatic, age-based policy for parental "proxy access" that violates Texas law by restricting parents' control over their minor-aged children's health records, effectively allowing a child to "own" their patient portal and potentially withhold information from their parents.	Press Release
Texas	Sony; Samsung; LG; Hisense; TCL	The AG alleged that these companies' use of automated content recognition technology to capture consumers' viewing habits and disclose that data for targeted advertising exposed consumers to privacy and security risks.	Press Release
Texas	General Motors, OnStar	The AG alleged that the company's telematics program did not disclose that the tool would collect, analyze, and transfer driving data for insurance purposes.	Press Release
Texas	TikTok	The AG alleged that the company misrepresented the nature and safety of its app by marketing it as appropriate for young users while knowingly exposing them to large volumes of sexual, violent, drug-related, and otherwise mature content and used an algorithmic feed intentionally designed to be highly addictive, maximizing time spent on the platform.	Complaint
Utah	Snap	The AG alleged that the company failed to inform consumers about its data collection practices and did not provide users or parents the ability to opt-out of the collection of sensitive data.	Complaint

If you have any questions, please contact us at info@fpf.org.

Disclaimer: This report is for informational purposes only and should not be used as legal advice.

1350 Eye Street NW Suite 350
Washington, DC 20005

info@fpf.org

FPF.org