Updates
December 20, 2024
Privacy Law Recap 2024: Regulatory Enforcement

This year saw significant enforcement activity from the Federal Trade Commission (FTC) on privacy, data security, and related technology topics, particularly with respect to location information, health, and other sensitive data; data brokers; children's privacy and online safety; and consumer protection issues related to artificial intelligence (AI). State privacy enforcers, such as Texas and California, were active as well, often in areas overlapping with federal enforcement. In this Update, we summarize highlights from the year and what to watch for in 2025.

FTC

Under the leadership of Chair Lina Khan, the FTC continued its assault on the "notice and choice" privacy framework, which was particularly evident in cases concerning sensitive data.

- **Location.** The FTC announced four significant settlements resolving allegations of unlawful collection, sale, and use of precise location information by data brokers (X-Mode, InMarket Media, Mobilewalla, and Gravy Analytics) and continued to pursue litigation against Kochava alleging similar conduct. Collectively, the four location settlements make clear that the FTC espouses the following principles:
    - Aggregations of data about the location of mobile devices are not anonymized because such information can be used to identify the owners of the devices—by buying data matching a device's mobile advertising ID to consumers' names and physical addresses or by using time-stamped signals to, for example, infer consumers' home addresses based on the device's nightly location.
    - Such information can be used to identify consumers' trips to sensitive locations, such as medical facilities.

- There must be affirmative consent to collect, use, or sell precise location information, and businesses who acquire it from third parties must take reasonable steps to verify that consumers authorized the downstream disclosure and use of their location information.

The consent orders in all four cases restrict the sale and/or use of precise location data about sensitive locations—such as medical facilities, religious organizations, and childcare facilities—and require a "sensitive location data program" to identify sensitive locations to prevent the disclosure and/or use of sensitive location information in line with the orders' other requirements. They also mandate the establishment of a supplier assessment program to confirm that consumers have provided appropriate consent to the processing of their precise location data.

- **Segments based on "sensitive characteristics."** In *Gravy Analytics*, *Mobilewalla*, and *X-Mode*, the FTC also challenged as unfair the categorization of consumers based on "sensitive characteristics," such as medical conditions, religious beliefs, and political activities, derived from location data, along with the sale or other transfer of such segments. According to the FTC, this practice, particularly by companies that consumers never interact with, is "far outside the expectations and experience of consumers" and exposes them to "risks of discriminatory treatment."
- **Health.** The FTC added to its recent line of cases concerning the collection and sale of health information for advertising purposes. In both *Monument Inc.* and *Cerebral, Inc.*, the FTC alleged that online services providing online mental health and/or substance abuse counseling services each disclosed sensitive health data to third-party advertising platforms via tracking technologies integrated into the businesses' websites and/or apps. According to the FTC, Monument's and Cerebral's respective failures to obtain consumers' affirmative express consent for the disclosure of their health information for advertising purposes were unfair under Section 5. Similarly, over the dissent of Commissioners Melissa Holyoak and Andrew Ferguson, the FTC expanded the Health Breach Notification Rule to apply to a broad range of health and wellness apps and to codify its view that a company's unauthorized disclosure of covered health information—such as for advertising—constitutes a "breach of security" under the rule.
- **Browsing data.** The FTC asserted that web browsing data is "sensitive. Full stop" in connection with its enforcement action in *Avast*. There, the FTC alleged that businesses offering antivirus software and browser extensions sold consumers' re-identifiable browsing data—such as search queries and the URLs of webpages they visited, tied to persistent identifiers—for advertising, marketing, and data analytics, which was unfair and deceptive.
- **Youth privacy and online safety.** Youth privacy and online content safety were a priority this year, too.
  - The FTC initiated an enforcement action against TikTok under the Children's Online Privacy Protection Act (COPPA), alleging that the video-sharing platform allowed children under 13 to bypass the company's age gate.
  - The agency announced a settlement with NGL Labs, LLC, an anonymous messaging app marketed to teens and children allegedly used to send threatening and sexually explicit content. The FTC alleged the defendants unfairly marketed the app to children and teens despite "knowing that use of anonymous messaging apps by these groups causes substantial injury" and touted the consent order's ban on offering anonymous messaging apps to children under 18. However, Commissioners Ferguson and Holyoak pushed back on the notion that offering anonymous messaging services for children and teens was necessarily unfair or that such a principle could be squared with the First Amendment.
  - The FTC released a staff report on the data practices of social media and streaming services, which criticized the widespread practice of treating teen and adult users alike, alleged that businesses "turn a blind eye" to the presence of users under 13, and highlighted concerns about the impact of social media use on the mental health of teens and children—a concern reflected in the FTC's proposed update to the COPPA Rule, which would limit companies' ability to nudge children and teens to stay

online.

- **Data security.** Data security is a perennial priority for the FTC, and in 2024, the agency announced several data security enforcement actions with novel theories. For example, in *Blackbaud*, the FTC brought its first standalone Section 5 unfairness claim for unreasonable data retention and both unfairness and deception claims for data breach notices that allegedly understated the scope and severity of the breach. In *Marriott*, though one of two data breaches into Marriott's Starwood subsidiary concluded *before* Marriott acquired Starwood, the FTC alleged that Marriott was responsible for this incident because in the due diligence process, it had "reviewed and evaluated Starwood's information security program to understand the state of Starwood's computer networks, systems, and their vulnerabilities, including the information security failures that led to the [breach]."
- **AI consumer protection enforcement.** The FTC began to announce enforcement actions concerning the conduct the FTC had warned of in a wave of blog posts about AI consumer protection issues. For example:
    - In *Evolv Technologies* and a law enforcement "sweep" called Operation AI Comply, the FTC announced a number of cases alleging that businesses exaggerated or failed to substantiate the AI-powered capabilities of their products and services. For example, the FTC alleged that Evolv made false or unsubstantiated claims to schools regarding the accuracy, effectiveness, and benefits of its AI-based weapons scanners.
    - Other activity concerned the use of AI to facilitate consumer deception. In *Rytr*, the FTC alleged that an AI-powered "writing assistant" provided the "means and instrumentalities" to generate fake product reviews by quickly generating an unlimited number of genuine-sounding product reviews containing details that have no relation to the user's input. Commissioners Ferguson and Holyoak dissented, emphasizing the need to demonstrate that Rytr knew or should have known that the writing assistant would be used for deceptive purposes and noting that the FTC's complaint did not supply a single example of someone having used Rytr's tool to violate Section 5. Similarly, the FTC proposed expansion of its new Impersonation Rule to reach AI-based platforms, software developers, and others that aid or facilitate rule violations by providing goods or services "with knowledge or reason to know that those goods or services will be used to" violate the rule, over the dissent of Commissioners Holyoak and Ferguson.

States

The priority areas in state enforcement actions largely mirrored those at the federal level. While California remained active, the big news was the breakout role of the Texas Attorney General in privacy enforcement.

Texas

Shortly after announcing the creation of a team dedicated to enforcement of a mixture of federal and state privacy laws, the Texas Attorney General announced a series of enforcement actions, including several utilizing recently enacted state laws:

- A $1.4 billion settlement to resolve allegations that Meta collected biometric data without informed consent in violation of Texas' Capture or Use of Biometric Identifier Act.
- A lawsuit against TikTok under the Securing Children Online Through Parental Empowerment Act, which went into effect September 1, 2024, alleging disclosure of known minors' personal information to third parties and to TikTok users without parental consent and without providing required parental controls.
- A settlement with Pieces, a company that uses generative AI to summarize patients' conditions and treatment for medical staff, to resolve allegations that the company misrepresented its product's accuracy rates and reliability.

- Letters to over 100 companies regarding their "apparent failure" to register as data brokers under the state's Data Broker Law, which went into effect on September 1, 2023.

Children's Privacy and Online Safety

The California Attorney General announced a settlement with Titling Point Media, resolving allegations that its mobile game was directed at children under 13, contained a nonneutral age gate, and collected and disclosed children's personal information in violation of COPPA and the California Consumer Privacy Act (CCPA).

A coalition of 14 state attorneys general led by California and New York sued TikTok under state unfair and deceptive acts and practices laws and COPPA, alleging that the service is harmful for young users' mental health and knowingly collects personal information of children under 13.

Data Brokers

Similar to Texas, the California Privacy Protection Agency announced an investigative sweep concerning data broker compliance with the registration requirements of the California Delete Act. A few weeks later, it announced settlements with Growbots, Inc. and UpLead LLC for allegedly failing to register and pay the annual data broker registration fee. Growbots agreed to pay $35,400 to resolve the claims, and UpLead agreed to pay $34,400.

Opt-Outs From the Sale of Personal Data

The California Attorney General announced a settlement with DoorDash (the office's second settlement under the CCPA) to resolve allegations that the company violated the CCPA and California Online Privacy Protection Act. As part of its involvement in a marketing cooperative, DoorDash allegedly provided personal information to the cooperative in exchange for the ability to advertise to customers of other participants in the cooperative. According to the California Attorney General, this constituted a "sale" under the CCPA, and DoorDash had not provided notice or an opportunity to opt out of that sale. Without admitting the allegations, DoorDash agreed to a $375,000 civil penalty to resolve the claims. The California Attorney General also announced an investigative sweep into streaming apps and devices to examine their compliance with the CCPA's opt-out requirements, including whether they provide an easy mechanism to opt out of the sale or sharing of personal information.

The Year Ahead

FTC

Next year will bring significant changes to the FTC. After the inauguration, Commissioner Ferguson will serve as the agency's chair, and the Republicans will have a majority following confirmation of President-elect Donald Trump's pick, Mark Meador, to fill the Commission seat currently held by Lina Khan (see here).

The change in leadership is almost certain to end the string of rulemakings under Section 18 of the FTC Act (also called "Magnuson-Moss") under the leadership of Chair Khan and put the nail in the coffin of the pending "Commercial Surveillance" rulemaking.

At the same time, since joining the FTC on April 2, 2024, Commissioner Ferguson has voted in support of a number of the agency's privacy and related enforcement actions, such as cases concerning children's privacy and online safety, location privacy, and data security, and we expect that the FTC's attention to these and other privacy and consumer protection technology issues will continue, adjusted to reflect the perspective of

Commissioner Ferguson and the Republican majority. For example, Commissioner Ferguson's statement on the Mobilewalla and Gravy Analytics cases suggests we may continue to see unfairness claims concerning the unlawful collection and sale of location data, whereas unfairness claims concerning the classification of consumers by sensitive characteristics derived from location data may be refashioned or omitted.

The FTC is also likely to explore new areas, such as how social media platforms engage in content moderation, about which Commissioner Ferguson has expressed concern. AI-related issues are likely to remain a priority, but Commissioner Ferguson has indicated a concern about the FTC "bend[ing] the law" in a rush to regulate AI. Thus, for AI, we are likely to see continued FTC reliance on theories about exaggerated and unsubstantiated claims about the capability of AI-powered products and fewer novel theories, such as those to render AI-powered software and platforms liable for deceptive or unfair practices by others (as under the FTC's proposed supplemental rule on AI impersonation) or application of Section 5 to allege that AI systems perpetuate discriminatory outcomes based on protected classes.

States

State enforcers will continue to be active, with eight comprehensive consumer privacy laws slated to come into effect in 2025 (Delaware, Iowa, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Tennessee), joining the eight laws already in force. We expect to see further attention to children's privacy and online safety, AI, automated decision-making, and perhaps the first enforcement action under the Washington My Health My Data Act. In addition, states will likely focus on transparency obligations, restrictions on targeted advertising and data "sales," and data security.

This post is part of a series recapping privacy law developments in 2024. Please see the following Updates for further information:

- Privacy Law Recap 2024: Data Security
- Privacy Law Recap 2024: State Consumer Privacy Laws

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law

Related insights

Update

FTC Brings First Standalone Section 5 Unfairness Claims for Unreasonable Data Retention and Inaccurate Breach Notice

Update

FTC Proposes Changes to COPPA Rule