Location Data And Online Tracking Trends To Watch

By **Emily Dorner, Jason Raylesberg and Kristina Iliopoulos** (August 11, 2025)

Emily Dorner

Jason Raylesberg

Kristina Iliopoulos

As the first half of 2025 underscored, regulators and class action plaintiffs are increasingly targeting companies' use of online tracking technologies and geolocation data in both privacy enforcement and litigation.

So far this year, there have been numerous developments, including:

- Consumers bringing the first federal class action complaint under the Washington My Health My Data Act;
- Honda and Todd Snyder entering into settlements with the California Privacy Protection Agency over privacy violations;
- The CPPA announcing an investigative sweep of the location data industry;
- The Connecticut Office of the Attorney General releasing an annual report on the enforcement of the Connecticut Data Privacy Act; and
- Texas Attorney General Ken Paxton bringing his first enforcement action under the state's broadly applicable consumer privacy law.

These developments reinforce the need for companies to periodically evaluate their compliance practices related to tracking technologies and the collection and use of location data. Because such technologies and practices are critical business tools, companies should create a process to implement them effectively and safely, with an eye to an evolving privacy-protective landscape.

We discuss each of these developments in detail below.

First Federal Class Action Under the My Health My Data Act

On Feb. 10, consumers filed a class action complaint against Amazon and Amazon Advertising LLC under the MHMDA.[1] The complaint, Maxwell v. Amazon.com Inc., filed in

the U.S. District Court for the Western District of Washington, was the first federal lawsuit brought under the MHMDA.

The MHMDA, itself a first-of-its-kind statute, broadly restricts how regulated entities may collect, share and sell consumer health data that is not protected under the Health Insurance Portability and Accountability Act or other privacy regimes, such as those governing the use of health data in some clinical trials.

The complaint alleges that Amazon unlawfully collected and monetized consumer geolocation data using certain online tracking technologies integrated into more than 10,000 Android and iPhone mobile applications.

Specifically, the plaintiff claims that Amazon's software development kit, which was embedded in these mobile applications, collected location data and ad IDs in violation of the MHMDA, as well as the Federal Wiretap Act, the Stored Communications Act, the Computer Fraud and Abuse Act, and certain common-law privacy claims.

Some of the geolocation data allegedly collected provides insights into a consumer's health, including visits to clinics, health behaviors like eating fast food or going to the gym, social determinants of health including the environment in which a consumer lives and works, and social networks that may influence health. The complaint does not contain details as to how the location data revealed health information about the individual plaintiff.

Amazon allegedly did not give notice of or obtain consumers' consent prior to the collection and sharing of this data, in violation of the MHMDA.

While similar state health privacy laws, like those in Connecticut and Nevada, do not contain a private right of action, the MHMDA provides that consumers who suffer injury from a violation of the statute may sue for damages under Washington's Consumer Protection Act.

To prevail on a CPA claim based on a violation of the MHMDA, a plaintiff must establish the underlying MHMDA violation, causation and damages, and a prevailing plaintiff may recover actual damages, costs of suit, reasonable attorney fees, and treble damages per plaintiff not to exceed $25,000.

First Enforcement Action Under Texas' Broad Consumer Privacy Law

The MHMDA lawsuit comes just a month after Texas Attorney General Ken Paxton announced his first enforcement action under the Texas Data Privacy and Security Act against Allstate and its subsidiaries, for allegedly collecting, using and selling the geolocation of drivers without proper notice and consent.[2]

In State of Texas v. The Allstate Corp., in the District Court ofMontgomery County, Texas, Allstate allegedly collected trillions of miles worth of location data from over 45 million consumers to create the "world's largest driving behavior database," which Allstate not only used for its own insurance underwriting but also sold to other insurers.

According to the complaint, insurers would use this data to justify increasing car insurance premiums or denying consumers' coverage.[3] Paxton claimed that Allstate violated the TDPSA and other laws by failing to provide a reasonably accessible privacy notice stating how consumers may exercise their rights under the TDPSA and to disclose material information about Allstate's practices with respect to targeted advertising and sales of personal data.

The enforcement action comes approximately six months after Paxton announced that he would initiate investigations into several car manufacturers after "widespread reporting that they have secretly been collecting mass amounts of data about drivers directly from their vehicles and then selling that data to third parties — including to insurance providers."[4]

California Regulator Actions

Honda's Settlement With the CPPA

On March 7, the CPPA issued a decision requiring American Honda Motor Co. to revise its privacy-related business practices and pay a $632,500 fine to resolve claims that Honda violated the California Consumer Privacy Act.[5]

Almost two years earlier, the CPPA announced that it was reviewing data privacy practices by connected vehicle manufacturers, which included Honda and ultimately led to the March decision.[6]

The CPPA found that Honda (1) sought too much personal information from consumers when they exercised their rights to opt out of Honda's sale of their personal information, of their personal information for cross-context behavioral advertising, or the use of their sensitive personal information for purposes not specified in the statute; and (2) made it difficult for consumers to use authorized agents to exercise their privacy rights.

The CPPA also found that Honda's online privacy management tool failed to offer privacy choices in a symmetrical manner. Specifically, Honda allegedly required consumers to go through two steps to opt out of the use of advertising cookies but only one step to accept the use of such cookies.

Citing the CCPA regulations, the decision reinforced that a choice for consumers regarding such uses and disclosures is not symmetrical if it requires more steps to opt out than to opt in. The CPPA further asserted that privacy-protective contracts were not in place with some of Honda's service providers that were accessing consumer personal data, including vendors providing online tracking tools.

In its settlement, Honda agreed to: (1) implement a new and simpler process for Californians to exercise their privacy rights; (2) certify its compliance, train its employees, and consult a user-experience designer to evaluate its methods for consumers to submit privacy-related requests; (3) change its contracting process to ensure appropriate mechanisms are in place to protect personal information; and (4) pay an administrative fine of $632,500.

Todd Snyder Settlement With the CPPA

On May 6, the CPPA issued a decision and order requiring clothing retailer Todd Snyder Inc., to change its privacy practices within 90 days and pay a $345,178 fine to resolve claims that the clothing retailer violated the CCPA.[7]

The CPPA found that Todd Snyder (1) failed to effectuate consumers' personal information opt-out preferences; (2) applied a verification standard for requests to opt out of sale and sharing of personal data; and (3) required consumers to submit more information than necessary to verify privacy rights requests.

As part of the order, Todd Snyder agreed to:

- Modify its current mechanism for enabling consumers to submit requests to opt-out of sale/sharing to ensure that it is not requiring consumers to provide more information than necessary or verify requests to opt-out of sale/sharing, as well as implement procedures to ensure that it appropriately processes requests and monitors the effectiveness/functionality of its methods for submitting opt-out requests;

- Not require consumers to provide more information than necessary to process a rights request;

- Develop, implement and maintain procedures to ensure that all personnel handling personal information are informed of the business' requirements under the CCPA;

- Maintain a contract management and tracking process to ensure that contractual terms required by the CCPA are in place; and

- Pay an administrative fine of $345,178.

Investigative Sweep of Location Data Industry

On March 10, California Attorney General Rob Bonta announced an investigative sweep into the location data industry. Bonta's office sent letters to advertising networks, mobile app providers and data brokers warning them about their obligations under the CCPA.[8]

The CCPA has special protections for data classified as sensitive, e.g., health or location data, including granting consumers the right to limit the use of sensitive personal data to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer.

For example, if a consumer exercises the right to limit a business' use of the consumer's sensitive personal data, the business may not exchange that data with nonvendor third parties.

Bonta noted that "location data is deeply personal, [it] can let anyone know if you visit a health clinic or hospital, and can identify your everyday habits and movements," and that businesses accordingly must take the responsibility to protect location data seriously, particularly in light of "the federal assaults on immigrant communities, as well as gender-affirming healthcare and abortion."

The Connecticut Attorney General's Annual Report on Enforcement of Consumer Privacy Law

Other state attorneys general are also taking action in response to inappropriate safeguards around the use of tracking technologies, e.g., cookies and pixels.

On April 17, the Connecticut Office of the Attorney General released an annual report on the enforcement of the Connecticut Data Privacy Act, or CTDPA.[9] The report provided an update on the office's broader privacy and data security efforts, consumer complaints received under the CTDPA to date, enforcement efforts, and expanded enforcement priorities.

Similar to the allegations made by the CPPA in its settlement with Honda, the Connecticut Office of the Attorney General issued cure notices to companies that allegedly failed to provide consumers with symmetrical choices to opt into and out of the use of cookies.

For example, one company investigated by the office allegedly used a cookie banner that enabled consumers only to opt in to the use of cookies by clicking on a button that read "accept all cookies." According to the report, the company included a link to "click here for more information," but that link brought consumers to the general privacy policy rather than offering an opportunity to opt out of the cookies.

The report explains that if a consumer is provided with a choice to accept all cookies by clicking a single button, they should also be provided a similar button to reject all cookies on the same screen, at the same time, and in the same color, font and size.

The office also enforced the CTDPA's prohibitions on processing consumer health data without affirmative consent and providing a processor with access to data without proper contracts in place. For example, the office sent a cure notice to a company that allegedly was transmitting sensitive health information to third parties via tracking technologies without sufficient consent.

Due to the cure notice, the company implemented an updated website user consent process, added consumer disclosures specific to Connecticut law, and conducted a data protection assessment for consumer health data.

Key Takeaways

The first federal MHMDA lawsuit, and the CPPA's and Texas attorney general's investigations, settlements and actions in the first half of 2025 indicate a continued litigation and enforcement focus on online tracking technologies and location data in particular.

Organizations should be vigilant in evaluating the manner in which they use tracking technologies on their website and within products, as well as their collection and use of geolocation data. Companies using tracking technologies should ensure that they, among other efforts:

- Provide consumers with clear and sufficient notice of the use of such data;

- Limit collection of such data to that reasonably necessary to perform the specific purposes for which the data is processed;

- Limit collection of information for purposes of verification in rights exercise;

- Regularly review and validate third-party privacy management tools to ensure proper functionality and compliance with applicable laws;

- Create processes for authorized agents to submit data subject requests;

- Obtain consent to and/or provide the right to opt out of the processing of sensitive information (including location data), depending on the jurisdiction; and

- Contractually require vendors to protect and limit their use of personal information in accordance with applicable law.

As enforcement around location data and tracking technologies becomes increasingly aggressive and multifaceted, organizations should view compliance as a dynamic, cross-functional responsibility — one that requires involvement from not only legal and privacy teams but also marketing, engineering, product development and procurement.

Regulators are scrutinizing not just the existence of privacy notices and opt-outs, but also how user choices are presented, processed and honored in practice. This means businesses must go beyond paper compliance and invest in operationalizing privacy through proactive measures such as regular audits and vendor due diligence.

Moreover, as states adopt divergent standards and enforcement strategies, companies operating nationally must adopt a scalable governance framework that can easily adapt to state-specific developments.

Emily Dorner and Jason Raylesberg are senior associates, and Kristina Iliopoulos is an associate, at Arnold & Porter Kaye Scholer LLP.

Arnold & Porter counsel Nancy Perkins and partner Jami Vibbert contributed to this article.

should not be taken as legal advice.

[1] https://www.law360.com/dockets/download/67ab37afc0ad7e8de2f01fd1?doc_url=https%3A%2F%2Fecf.wawd.uscourts.gov%2Fdoc1%2F197111622946&label=Case+Filing.

[2] https://www.oag.state.tx.us/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

[3] https://www.oag.state.tx.us/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf.

[4] https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-opens-investigation-car-manufacturers-collection-and-sale-drivers-data.

[5] https://cppa.ca.gov/regulations/pdf/20250307_hmc_order.pdf.

[6] https://cppa.ca.gov/announcements/2023/20230731.html.

[7] https://cppa.ca.gov/pdf/20250501_snyder_order.pdf.

[8] https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-investigative-sweep-location-data-industry.

[9] https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf.