

Location Data as Health Data? Precedent-Setting Lawsuit Brought Against Retailer Under Washington’s My Health My Data Act

February 20, 2025

By [Benjamin W. Perry](#), [Lauren N. Watson](#), and [Zachary V. Zagger](#)

An online retailer was recently hit with the first class action under Washington’s consumer health data privacy law alleging that it used advertising software attached to certain third-party mobile phone apps to unlawfully harvest the locations and online marketing identifiers of tens of millions of users. This case highlights how seemingly innocuous location data can become sensitive health information through inference and aggregation, potentially setting the stage for a flood of similar copycat lawsuits.



- An online retailer was hit with the first class action under Washington State’s My Health My Data Act (MHMDA), claiming that the retailer unlawfully harvested sensitive location data from users through advertising software integrated into third-party mobile apps.
- The lawsuit alleges that the retailer did not obtain proper consent or provide adequate disclosure regarding the collection and sharing of consumer health data; a term that is defined incredibly broadly as personal information that is or could be linked to a specific individual and that can reveal details about an individual’s past, present, or future health status.
- This case marks the first significant test of the MHMDA and could provide a roadmap for litigants in Washington and other states.

On February 10, 2025, Washington resident Cassandra Maxwell filed a class action lawsuit in the U.S. District Court for the Western District of Washington alleging violations of Washington’s MHMDA. The suit alleged that the retailer’s advertising software, known as a “software development kit,” or SDK, is licensed to and “runs in the background of thousands of mobile apps” and “covertly withdraws sensitive location data” that cannot be completely anonymized.

“Mobile users may agree to share their location while using certain apps, such as a weather app, where location data provides the user with the prompt and accurate information they’re seeking,” the suit alleges. “But that user has no idea that [the online retailer] will have equal access to sensitive geolocation data that it can then exfiltrate and monetize.”

The suit brings claims under federal wiretap laws, federal and state consumer protection laws, and violations of the MHMDA, making it a likely test case for consumer privacy claims under the MHMDA. This case evokes parallels to the surge over the past several years of claims under the [California Invasion of Privacy Act \(CIPA\)](#), a criminal wiretap statute. Both involve allegations of unauthorized data collection and sharing facilitated by digital tracking technologies. These technologies, including cookies, pixels, and beacons, are often embedded in websites, apps, or marketing emails, operating in ways that consumers may not fully understand or consent to.

As we [previously covered](#), hundreds if not thousands of lawsuits relating to similar technologies were brought pursuant to CIPA after a California district court denied a motion to dismiss such claims in *Greenley v. Kochava, Inc.* Given the parallels and the onslaught of litigation that CIPA entailed, the MHMDA case may set important precedents for how consumer health data privacy is interpreted and enforced in the digital age, similar to the impact CIPA litigation has had on broader privacy practices. Like CIPA, the MHMDA also allows for the recovery of attorneys’ fees, but unlike CIPA (which provides for statutory damages even without proof of actual harm), a plaintiff must prove an “injury” to his or her business or property to establish an MHMDA claim.

Consumer Health Data

As many companies working in the retail space likely know, the MHMDA imposes a host of new requirements for companies doing business in Washington or targeting Washington consumers with respect to the collection of “consumer health data.” The law broadly defines “consumer health data” as any personal information that can be linked or reasonably associated with an individual’s past, present, or future physical or mental health status. The MHMDA enumerates an entire list of data points that could constitute “health status,” including information that would not traditionally be thought of as indicative of health, such as:

- biometric data;
- precise location information that could suggest health-related activities (such as an attempt to obtain health services or supplies);
- information about bodily functions, vital signs, and symptoms; and
- mere measurements related to any one of the thirteen enumerated data points.

Critically, even inferences can become health status information in the eyes of the MHMDA, including inferences derived from nonhealth data if they can be associated with or used to identify a consumer’s health data.

For instance, Maxwell’s suit alleges the retailer collected her biometric data and precise location information that could reasonably indicate an attempt to acquire or receive health services or supplies. However, the complaint is light on factual support, alleging only that the data harvesting conducted via the retailer’s SDK *could* reveal (presumably via inference in most cases) “intimate aspects of an individual’s health,” including:

- visits to cancer clinics;
- “health behaviors” like visiting the gym or fast food habits;
- “social detriments of health,” such as where an individual lives or works; and
- “social networks that may influence health, such as close contact during the COVID 19 pandemic.”

Notice and Consent

The suit further alleges that the retailer failed to provide appropriate notice of the collection and use of the putative class members’ consumer health data and did not obtain consent before collecting and sharing the data. These allegations serve as a timely reminder of the breadth and depth of the MHMDA’s notice and consent requirements.

Unlike most other state-level privacy laws, which allow different state-mandated disclosures to be combined in a single notice, the Washington attorney general has indicated in (nonbinding) guidance that the MHMDA “Consumer Health Privacy Policy must be a separate and distinct link on the regulated entity’s homepage and

may not contain additional information not required under the My Health My Data Act.” Said differently, businesses in Washington cannot rely upon their standard privacy policies, or even their typical geolocation consent pop-up flows with respect to consumer health data.

Additionally, at a high-level, the MHMDA contains unusually stringent consent requirements, demanding the business obtain “freely given, specific, informed, opt-in, voluntary, and unambiguous” consent before consumer health data is collected or shared for any purpose other than the provision of the specific product or service the consumer has requested from the business, or collected, used, or shared for any purpose not identified in the business’s Consumer Health Privacy Policy.

Next Steps

The *Maxwell* lawsuit is significant as it is the first to be filed under Washington’s MHMDA, a law that has already spawned a copycat law in Nevada, a lookalike amendment to the Connecticut Data Privacy Act, and a whole host of similar bills in state legislatures across the country—most recently in New York, which has its own version of the MHMDA awaiting presentation to the governor for signature. The suit appears to take an expansive interpretation that could treat nearly all or essentially all location data as consumer health data, inasmuch as conclusions about an individual’s health that can be drawn from the data. And, while the MHMDA does use expansive language, the suit appears likely to answer still lingering questions about the extent of what should be considered “consumer health data” subject to the rigorous requirements of the MHMDA.

As this suit progresses, companies targeting Washington consumers or otherwise doing any business in Washington may want to review their use of SDKs or similar technologies, geolocation collection, and any other collection or usage of consumer data with an eye toward the possibility that the data could be treated as consumer health data. Also, their processors may wish to do the same (remember, the Washington attorney general has made it clear that out-of-state entities acting as processors for entities subject to MHMDA must also comply). Depending on what they find, those companies may wish to reevaluate the notice-and-consent processes applicable to the location data they collect, as well as their handling of consumer rights applicable to the same.

Ogletree Deakins’ [Cybersecurity and Privacy Practice Group](#) will continue to monitor developments and will provide updates on the [Cybersecurity and Privacy, Retail](#), and [Washington](#) blogs.

Follow and Subscribe

[LinkedIn](#) | [Instagram](#) | [Webinars](#) | [Podcasts](#)



[Benjamin W. Perry](#)

Shareholder, [Nashville](#)



[Lauren N. Watson](#)

Associate, [Raleigh](#)



[Zachary V. Zagger](#)

Senior Marketing Counsel, [New York](#)

TOPICS

[Cybersecurity and Privacy](#) , [Retail](#) , [State Developments](#) , [Washington](#)

RELATED ARTICLE



February 20, 2025

[‘What Is a Woman?’ Alabama Governor Signs Bill Declaring There Are Only Two Sexes](#)

RELATED PODCAST



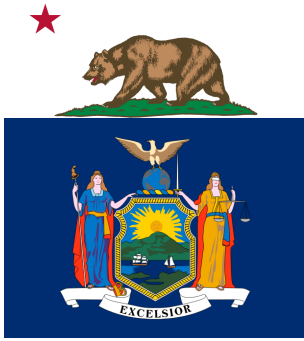
December 16, 2024

[The AI Workplace: Illinois’s AI Employment Law, HB 3773, Explained](#)

RELATED ARCHIVED WEBINARS

February 20, 2025

[California Coffee Talk: R-E-S-P-E-C-T—Find Out What It Means for Your Workplace](#)



January 21, 2025

New York's Groundbreaking Paid Prenatal Leave Law: How to Prepare