Published on *The National Law Review* https://natlawreview.com

First Class Action Filed Under Washington's MY Health MY Data Act Draws Parallels to Previous SDK Litigation

Article By:

Ryan D. Ellard

On February 10, 2025, the first class action complaint was filed pursuant to Washington's MY Health MY Data Act ("**MHMDA**"), Wash. Rev. Code Ann. § 19.373.005 *et seq. See Maxwell v. Amazon.com*, Inc. et al., Case No. 2:25-cv-261 (W.D. Wash.). Broadly, the lawsuit alleges that, by using software development kits ("**SDKs**"), defendants Amazon.com, Inc. and Amazon Advertising, LLC harvested the location data of tens of millions of Americans without their consent and used that information for profit. The Complaint's core allegations in that regard are akin to previous SDK class actions, but the MHMDA claim is new.

Software Development Kits:

The Maxwell lawsuit focuses on an SDK allegedly licensed by Amazon to a variety of mobile applications. SDKs are bundles of pre-written software code used in mobile and other applications. Many SDKs include code required in virtually every app: APIs, code samples, document libraries, and authentication tools. Rather than writing code from scratch, developers often license SDKs to streamline the app development process. In theory, SDKs allow developers to build apps in a fast and efficient manner. However, many SDKs also gather user information, including location data.

The MY Health MY Data Act:

The MHMDA came into effect on March 31, 2024, and regulates the collection and use of "consumer health data." The term is broadly defined as personal information linked or reasonably linkable to a consumer and identifies the consumer's physical or mental health status, including "[p]recise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies." Wash. Rev. Code Ann. § 19.373.010. Among other things, regulated entities must provide consumers with a standalone consumer health data privacy policy; adhere to consent and authorization requirements; refrain from prohibited geofencing practices; comply with valid consumer requests; and enter into certain agreements with their processors. Unlike some other relatively similar state laws, the MHMDA includes a broad private right of action.

The Complaint:

Plaintiff Cassaundra Maxwell alleges that Amazon's SDKs, operating in the background of other

applications like the Weather Channel and OfferUp apps, unlawfully obtained user location data without consumers' knowledge or consent. More specifically, Plaintiff claims that "Amazon collected Plaintiff's consumer health data, including biometric data and precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies" without sufficient notice or consent. Plaintiff further asserts that, once the data was harvested, Amazon used it for its own targeted advertising purposes and for sale to third parties.

Plaintiff seeks to certify a class consisting of all natural persons residing in the United States whose mobile device data was obtained by Defendants through the Amazon SDK. The Complaint includes seven purported causes of action: (1) Federal Wiretap Act violations, (2) Stored Communications Act violations, (3) Computer Fraud and Abuse Act violations, (4) Washington Consumer Protection Act violations, (5) MHMDA violations, (6) invasion of privacy, and (7) unjust enrichment.

Historical Perspective:

Despite the new MHMDA claim, the *Maxwell v. Amazon* Complaint is similar to those from prior SDK cases. In *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023), for example, California residents brought a putative class action alleging improper data collection and dissemination by data broker Kochava. Similar to the *Maxwell* case, the plaintiffs in Greenley claimed that Kochava developed and coded its SDK for data collection and embedded it in third-party apps. They claimed the SDK secretly collected app users' data, which was then packaged by Kochava and sold to clients for advertising purposes. Much like the *Maxwell* litigation, the improper interception and use of location data was a focal point of the *Greenley* plaintiffs' allegations. Whereas the action against Amazon relies on the MHMDA, other Washington state law, and federal statues, the *Greenley* plaintiffs' claims were rooted in alleged violations of California state law, including the California Computer Data Access and Fraud Act (CDAFA), California Invasion of Privacy Act (CIPA), and California Unfair Competition Law (UCL). In *Greenley*, Defendants filed a motion to dismiss, arguing *inter alia* that Plaintiff lacked standing. The Court denied the motion, holding that, "[T]he Complaint plausibly alleges Defendant collected Plaintiff's data" and "there is no constitutional requirement that Plaintiff demonstrate lost economic value." *Greenley v. Kochava, Inc.,* 684 F. Supp. 3d 1024 (S.D. Cal. 2023).

Although the facts vary, some recent cases suggest courts may still be receptive to lack of standing arguments under certain circumstances. In a class action in the Southern District of New York, plaintiff claimed Reuters unlawfully collected and disclosed IP address information. *Xu v. Reuters News & Media Inc.*, 1:24-cv-2466 (S.D.N.Y.). Plaintiff alleged violations of the California Invasion of Privacy Act. The Court dismissed Plaintiff's claims for lack of standing, holding that the IP address used by Plaintiff to visit Reuters' website does not constitute sensitive or personal information. *Xu v. Reuters News & Media Inc.*, No. 24 CIV. 2466 (PAE), 2025 WL 488501 (S.D.N.Y. Feb. 13, 2025). The Complaint included no allegations of physical, monetary, or reputational harm. The Court noted that Plaintiff did not claim he received any targeted advertising (much less that he was harmed by such advertising) or that Reuters collected sensitive or personal identifying information data that could be used to steal his identify or inflict similar harm. *See also Gabrielli, v. Insider, Inc.*, No. 24-CV-01566 (ER), 2025 WL 522515, at *4 (S.D.N.Y. Feb. 18, 2025) (holding that, "Not only does an IP address fail to identify the actual individual user, but the geographic information that can be gleaned from the IP address is only as granular as a zip code.")

Takeaways:

Although the *Maxwell* Complaint against Amazon relies on the recently enacted MHMDA, its

underlying allegations largely track previous SDK claims. As states continue to enact privacy legislation granting private rights of action, businesses should expect to see SDK complaints repackaged to fit the confines of each statute. Until courts sort through these types of claims over the course of the next several years, we may see many more cases follow in *Maxwell's* footsteps. Businesses, particularly those in the healthcare space, should be mindful about their use of SDKs going forward.

National Law Review, Volume XV, Number 63