Unpacking First Consumer Claim Under Wash. Health Data Act

By **Starr Turner Drum and Alexander Altman** (March 14, 2025)

Starr Turner Drum

Alexander Altman

Almost one year after going into effect, the Washington My Health My Data Act has seen its first consumer class action claim: Maxwell v. Amazon.com Inc., in the U.S. District Court for the Western District of Washington.

Should the case make it to the dismissal stage and onward, the court will be confronted with questions of statutory interpretation that attorneys in counseling and litigation roles have been contending with since the MHMDA was first introduced.

MHMDA Background

The MHMDA is the first privacy law of its kind in the U.S., imposing obligations on a wide range of regulated entities that collect consumer health data, that is, according to the act, "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."[1]

Like the wave of general consumer privacy laws passed in the U.S., "personal information" under the MHMDA is broadly construed to include data points such as cookie IDs and IP addresses.[2] Applying to a broad range of regulated entities, it is a stated purpose of the MHMDA to close the gap between consumer expectations and the limited scope of the Health Insurance Portability and Accountability Act, which applies to only a narrow category of entities.[3]

Among other obligations, the MHMDA requires regulated entities to (1) provide consumers a specific consumer health data privacy policy, (2) obtain consent for the collection — and certain disclosures of — consumer health data, and (3) obtain a written and signed HIPAA-style authorization for any sale of consumer health data.

Crucially, and unlike almost all consumer privacy laws in the U.S., the MHMDA provides aggrieved consumers a private right of action, in this case by way of Washington's Consumer Protection Act.[4] Although the Consumer Protection Act does not include allow for recovery of liquidated or statutory damages, claimants can seek actual damages, which the court may treble up to $25,000 per violation.[5]

Key Maxwell Allegations

The Maxwell complaint alleges that defendants Amazon.com Inc. and Amazon Advertising LLC (collectively Amazon) improperly collected Maxwell's and other putative class members' data by way of its software development kit, which it licensed to third-party app developers.[6]

As a result, Maxwell alleges that Amazon profited from the collection of this data "both for its own targeted advertising methods and by selling the data to others looking to help their own bottom line."[7] Specifically, the complaint alleges 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 the requisite notice or consent.[8]

The complaint does not contain allegations that Amazon sold Maxwell's consumer health data without the requisite signed authorization.

The MHMDA claim in Maxwell comes alongside a number of wiretapping-related claims that have become common in the privacy litigation landscape over the past few years, including under the Federal Wiretap Act,[9] the Stored Communications Act,[10] the Computer Fraud and Abuse Act,[11] and various state wiretapping statutes.

In this vein, Maxwell coincides with at least two other cases recently filed against Amazon — Albano v. Amazon Inc. in the Western District of Washington, and Kolotinsky v. Amazon.com Inc., in the U.S. District Court for the Northern District of California — in connection with its collection of consumer data through licensed software development kits. Both of these cases bring various wiretapping claims, but no claims under the MHMDA.[12]

Model Case? Or Not the Right Fit?

The MHMDA claim in Maxwell faces a few potential hurdles. First, Amazon may not be the right defendant to target under the MHMDA, at least from a substantive perspective. The MHMDA, in relevant part, requires regulated entities to provide privacy policies describing how they collect consumer health data and obtain consumer consent to collect such data.

As alleged in the complaint, Amazon arguably did not perform the "collection" necessary to trigger liability under the MHMDA. Rather, Amazon's software development kit appears to have been licensed and deployed by third-party app developers, who are seemingly the entities that would have actually collected consumer health data and, through the software development kit, allegedly disclosed the data to Amazon.

Notably, no mobile app developers are named in the suit. In bringing the claim against Amazon, the plaintiff in Maxwell seemingly advances a kind of aider-and-abettor liability under the MHMDA. Neither the MHMDA nor the Consumer Protection Act, however, appear to contemplate such imputed liability.

Notably, the typical wiretapping claims brought alongside the MHMDA claim proceed under a direct theory of liability, i.e., that the defendant itself is an intruder or eavesdropper. The Federal Wiretap Act, for example, prohibits the "intentional interception" of communications.[13] Similarly, the Computer Fraud and Abuse Act prohibits a person from "intentionally access[ing] without authorization" or "intentionally exceed[ing] an authorization to access" an electronic communications service.

In essence, the allegations look like an attempt to fit an MHMDA "peg," i.e., collection, into a wiretapping "hole," i.e., eavesdropping. Should Maxwell make it to the dismissal stage, the court may be tasked with determining what it means to be the collector of consumer health data under the MHMDA.

If the MHMDA claim in Maxwell advances past dismissal, it may face another issue of statutory interpretation at the class certification stage. The complaint alleges only one class: "All natural persons residing in the United States whose Mobile Device Data was obtained by Defendants through the Amazon Ads SDK."[14]

There is no Washington State subclass. This raises the question of whether non-

Washingtonians are entitled to relief under the MHMDA. Most of the general consumer privacy laws in the U.S. are fairly clear in that they apply only to the residents of those states.[15] The MHMDA's definition of "consumer," however, has a peculiar twist. Not only does it cover Washington residents; it also includes "a natural person whose consumer health data is collected in Washington."[16]

If a nationwide class were to be certified for the MHMDA claim, therefore, the court would likely need to find that the consumer health data of non-Washington residents was collected in Washington by virtue of using mobile apps incorporating Amazon's software development kit. In other words, to certify a nationwide class for the MHMDA claim, Maxwell will have to find another Washington hook. In this case, that hook could be Maxwell's allegations that both defendants have a principal place of business in Seattle, Washington.[17] Whether this will be enough for the court to conclude that consumer health data was collected in Washington remains to be seen.

Finally, the complaint may lack specificity under the Supreme Court cases Bell Atlantic v. Twombly and Ashcroft v. Iqbal, decided in 2007 and 2009, respectively, to sustain the MHMDA claim. For example, Maxwell does not allege which, if any, mobile apps they used that incorporated Amazon's software development kit, making it difficult to understand the extent of consumer health data allegedly collected.

What Does the Future Hold for MHMDA Claims?

As mentioned above, the MHMDA is relatively unique in providing consumers a private right of action. Few other U.S. consumer privacy laws grant aggrieved consumers this relief. And unlike some other consumer privacy laws, the MHMDA entitles litigants only to actual, not statutory, damages, which are notoriously difficult to prove in privacy litigation and may make the MHMDA less amenable to class action certification.

With this limitation weighing the MHMDA's private right of action down to begin with, Maxwell's unique allegations and theory of liability may not be able to trigger an aftershock of similar claims.

Nevertheless, the MHMDA's first private claim may yield insight to litigators and compliance counsel should the court take the opportunity to interpret some of the statute's more opaque language. Then again, Maxwell could settle before any of the more interesting issues are decided, creating nothing more than a faint rumble in the privacy litigation landscape.

Starr Turner Drum is a shareholder and Alexander S. Altman is counsel at Polsinelli PC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] RCW 19.373.010(8)(a).

[2] See id. 19.373.010(18)(a).

[3] See id. 19.373.005(2).

[4] See RCW Chapter 19.86.

[5] See RCW 19.86.090.

[6] Complaint, Maxwell v. Amazon.com Inc. et al., Dkt. No. 1 (W.D. Wash. Feb 10, 2025), ¶¶ 3-5 ("Compl.").

[7] Id. ¶ 6.

[8] Id. ¶¶ 132-133.

[9] 18 U.S.C. § 2510, et seq.

[10] 18 U.S.C. § 2701.

[11] 18 U.S.C. § 1030.

[12] See Complaint, Albano et al. v. Amazon Inc., et al, Case No. 2:25-cv-00252, Dkt. No. 1 (W.D. Wash. Feb. 7, 2025) (alleging, inter alia, violations of FWA, CFAA, California Invasion of Privacy Act (Cal. Pen. Code § 631) ("CIPA")); Complaint, Kolotinsky v. Amazon.com Inc. et al, Case No. 25-00931, Dkt. No. 1 (N.D. Cal. Jan. 29, 2025) (alleging violations of CIPA, California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502)).

[13] 18 U.S.C. § 2511(1)(a).

[14] Compl. ¶ 43.

[15] See, e.g., Cal. Civ. Code § 1798.140(i) (defining "consumer" as "a natural person who is a California resident"); Colo. Rev. Stat. § 6-1-1303(6)(a) (defining "consumer" as "an individual who is a Colorado resident acting only in an individual or household context.").

[16] RCW 19.373.010(7).

[17] Compl. ¶¶ 9-10.