The Privacy Map Expands: Michigan Emerges in Website Tracking Litigation

February 18, 2026

A putative class action against Blue Cross Blue Shield of Michigan (BCBSM) has been filed in the Eastern District of Michigan alleging that commonplace website tracking and session replay tools violate both federal and Michigan wiretap and eavesdropping laws. The case, *Falls v. Blue Cross Blue Shield of Michigan Mutual Insurance Company*, joins nearly 4,000 others that have been filed across the U.S. since 2022 alleging some form of wiretapping based on website interactions.

What Happened?

In *Falls*, plaintiffs allege that BCBSM deployed third-party tracking pixels on its public-facing websites that collected and transmitted visitors' personally identifiable information to outside technology vendors without adequate notice or consent. According to the complaint, the challenged tracking technologies allegedly captured information tied to users' interactions with BCBSM's website and shared that data with third parties for analytics and advertising purposes.

The case underscores that even heavily regulated entities in the healthcare sector are facing litigation involving allegations directed at standard website analytics tools, independent of any alleged data breach or cybersecurity incident. The claims are purportedly brought under the Federal Wiretap Act (18 U.S.C § 2510 et seq.) and the Michigan Eavesdropping Statute (MCL 750.539a et seq.).

Two Cases – A Trend?

This lawsuit joins *Goodman v. Hillsdale College*, a recently settled class action lawsuit brought in the Western District of Michigan. In the case, the Court denied Hillsdale College's motion to dismiss a putative class action alleging violations of the Video Privacy Protection Act (VPPA) based on the college's use of website tracking technology on its online lecture platform. The *Hillsdale* decision rejected the notion that nonprofits or mission-driven organizations are exempt from privacy statutes like the VPPA. The court made clear that free content, educational purpose, and nonprofit structure do not preclude liability where statutory elements are plausibly alleged.

Why This Matters

Digital wiretapping litigation has surged sharply in recent years, driven largely by lawsuits challenging the use of website tracking technologies such as cookies, pixels, session-replay tools, and chat features. Nearly 4000 digital wiretapping lawsuits have been filed across the U.S. since mid-2022. While California remains the epicenter, the data show a rapid geographic expansion, with filings increasing in states such as Florida, Pennsylvania, and Massachusetts, reflecting a growing plaintiffs' bar targeting consumer-facing businesses nationwide for alleged violations of state and federal wiretap statutes based on routine digital analytics and marketing practices. These cases are often pled as putative class actions and seek statutory damages, attorneys' fees, and injunctive relief.

Key Takeaways for Organizations

- Plaintiffs' firms are actively scanning websites for tracking technologies that can form the basis of statutory claims.
- Consent defenses are winning but cookie banners, consent tools, and privacy disclosures must align with actual data flows, not just stated policies.[i]

Continued

- Nonprofits, educational institutions, and mission-driven organizations face the same scrutiny as commercial entities.

If you have questions about how this increase in litigation may impact your business, contact your Miller Canfield attorney or a member of Miller Canfield's Advertising and Marketing Team.

[i] *Lakes v. Ubisoft, Inc.*, 777 F. Supp. 3d 1047 (N.D. Cal. Apr. 2, 2025)