Insights, News & Events

ANOTHER DIGITAL WIRETAPPING WIN IS GOOD NEWS FOR BUSINESSES: WHAT YOU NEED TO KNOW ABOUT PENNSYLVANIA DECISION

Insights
Apr 7, 2026

Another Digital Wiretapping Win is Good News for Businesses: What You Need to Know About Pennsylvania Decision

In an important decision for businesses fighting state wiretapping claims based on website activity, the 3rd Circuit recently said that federal courts lacked jurisdiction to hear a case under Pennsylvania's wiretapping law. The case involves a consumer who alleged that her data was collected without her knowledge or consent by a website owner and a website analytics company. The court's March 24 decision, however, found that she did not suffer a cognizable harm sufficient to avail herself of federal jurisdiction and upheld the case's dismissal. In this Insight, we provide you with a summary of the case and some best practices to defend your business against wiretapping laws.

What's at Issue?

Recent litigation across the country has targeted businesses that use session replay, third-party tracking, pixel tracking, and cookies on their website. Courts have recognized that these technologies may constitute unlawful interception if implemented without proper consent.

We track these lawsuits on our Digital Wiretapping Litigation Map, and you can see that California holds the lead with the most lawsuits filed under its wiretapping statute (CIPA). However, opportunistic attorneys have applied the same strategy in other states, with Pennsylvania and Florida

Related People

Risa B. Boerner, CIPP/US, CIPM

Partner

610.230.2132

Catherine M. Contino

Associate

seeing a large uptick in class action lawsuits alleging violations of wiretapping cases that involve website cookies, pixels, and trackers.

What is WESCA?

The Pennsylvania Wiretapping and Electronic Surveillance Control Act (WESCA) broadly prohibits the intentional interception, disclosure, or use of wire, electronic, or oral communications without the consent of all parties. It has three key provisions:

- **Private Right of Action**: Individuals may sue for actual damages or liquidated damages up to $1,000 (whichever is higher), punitive damages, and reasonable attorneys' fees. Given the significant statutory damages available under WESCA, plaintiffs are incentivized to file suit, especially as a class action.
- **All-Party Consent**: WESCA requires consent of all parties to a communication for lawful interceptions or recording, which aligns with Florida, California, and Massachusetts. This means that for communications in these states, explicit or implied consent is required, whether it is a phone call, email, or website interactions. It is difficult to apply these to digital communications, such as those involve website interactions.
- **Exceptions**: WESCA provides exceptions for law enforcement with prior approval and public settings where there is no expectation of privacy. These exceptions are narrowly construed and have yet to be applied in a digital context.

Recent case law has applied WESCA to modern technology, repurposing a statute originally meant to apply to telephones to address internet and digital-based privacy violations.

What Happened in This Case?

Plaintiff Ashley Popa alleges she visited the Harriet Carter Gifts website looking for pet stairs, but never made a purchase. Popa alleged that the code on the website placed third-party cookies on her browser that allowed a third-party marketing service, NaviStone, to track her website interactions for the purpose of delivering mail advertisements. She alleged a violation of WESCA, arguing

610.230.6109

Service Focus

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

that both the website owner and the analytics service used tracking technology without her consent or knowledge.

The court ruled for defendants and Popa appealed. While the appeal was pending, the court decided *Cook v. GameStop*, holding that a plaintiff who merely moves her mouse, clicks on links, searches the website via search bar, and adds a product to a digital shopping cart did not share any sensitive personal information – and therefore did not suffer a concrete injury in fact to establish standing.

Just as in that case, the court found that Popa did not suffer harm sufficient to establish "standing" and form a basis for federal subject matter jurisdiction. Therefore, the court once again ruled for the defendants.

What is Standing?

Article III of the US Constitution limits federal courts to hearing only "cases" or "controversies." In simple terms, not everyone who is upset about something can sue in federal court – there are specific requirements. To have standing, a person must show three things:

1. Injury: You must have suffered, or will soon suffer, a real and specific harm. This harm can be physical, financial, or even a violation of your rights, but it can't be just a general complaint about the law or government.

2. Causation: The harm you suffered must be directly linked to the actions of the person or group you are suing. In other words, your injury must be caused by what the defendant did (or didn't do).

3. Redressability: The court must be able to do something to fix your injury. If the court's decision can't help you, then you don't have standing.

What Did the Court Decide and Why is it Important?

Although this decision represents a victory for businesses, claims of wiretapping by website visitors can be significant for small and medium-sized businesses with limited financial resources to fight. In addition, these types of claims are often brought by the same plaintiffs – called "testers" – calling into question whether these types of suits are really for the purpose of consumer advocacy or are just the latest trend for opportunistic plaintiffs' lawyers.

Moreover, even though this case resulted in a win for defendants, it does not eliminate all risk. Plaintiffs' claims may still proceed in state court, and businesses remain exposed to costly class action litigation over cookies, pixels, session replay, and other tracking technologies.

Recommendations for Businesses

- Review your website's use of third-party cookies, pixels, session replay tools, and analytics vendors to understand what data is collected, who receives it, and whether that collection is adequately disclosed.
- Reassess consent mechanisms, privacy notices, and cookie disclosures, especially in all-party consent states such as Pennsylvania, California, and Florida.
- Evaluate vendor contracts and data-sharing arrangements to ensure third-party tools are appropriately governed, limited in scope, and aligned with your public disclosures.
- Develop a litigation-readiness plan that includes technical audits, records of consent flows, and coordination among legal, privacy, marketing, and IT teams so you can respond quickly if a wiretapping claim is filed.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber team.