Prepare For Pa. Consumer Suits After Website Wiretap Ruling

By **Thomas DeCesar and Jonathan Vaitl** (October 18, 2022)

Thomas DeCesar

Jonathan Vaitl

Browser cookies might not come to mind when most people think of wiretapping, but after a recent decision[1] out of the U.S. Court of Appeals for the Third Circuit, they are squarely in focus for a crop of new consumer class actions related to session replay software.

At issue in Popa v. Harriet Carter Gifts Inc. was an exception to Pennsylvania's Wiretapping and Electronic Surveillance Control Act, or WESCA,[2] that Pennsylvania courts had applied for years.

Under WESCA, it is unlawful to intentionally intercept any wire, electronic or oral communication.[3] Pennsylvania courts, however, have applied a direct party exception to WESCA, finding that a party who directly receives a communication does not "intercept" it. [4]

This limited the scope of potential claims under WESCA, which provides a direct cause of action for consumers. In 2012, the Pennsylvania General Assembly revised WESCA to modify the definition of "intercept" and specifically excluded communications directly received by law enforcement if certain criteria — oversight from a district attorney or the attorney general — were met. [5]

In Popa, the Third Circuit determined that, by enacting the 2012 revisions to WESCA, the general assembly limited the scope of the direct party exception to only those circumstances described in the statute — limiting its applicability to the law enforcement context and opening the door to consumer class actions claiming that internet tracking violates WESCA.

At least 11 consumer class actions alleging claims under WESCA have been filed[6] in the federal courts in Pennsylvania in the few weeks following the Third Circuit's decision.

The complaints allege that the defendants' websites use computer code — frequently referred to as session replay code — to intercept and record a website visitor's electronic communications, e.g., mouse movements, clicks, keystrokes, etc., with the defendants' websites in violation of WESCA.

These types of cases are not necessarily new or unique to Pennsylvania. For example, plaintiffs in California[7] and New York[8] have brought similar claims under the federal wiretapping statute.[9]

In the New York action, for instance, the plaintiff brought claims against online consumer retailers, as well as a marketing company and data broker that had embedded code on the retailers' websites to track and record mouse clicks, items added to carts, and even form data that was not submitted.

However, in its decision dismissing the plaintiff's complaint for failure to state a claim, the U.S. District Court for the Southern District of New York pointed out that the federal wiretapping statute is a one-party consent law, meaning that as long as one of the parties to the communication has consented to the recording, there is no interception.[10]

As a result, the court held that the plaintiff had failed to state a claim because the retailers were a party to the communication, and the marketing company recording the data had their consent.

Pennsylvania, by contrast, along with several other states — California, Delaware and Florida — is a two-party consent state, which means that every party to a communication must consent to a recording. Because of this distinction, consent becomes a critical consideration for cases brought under WESCA.

In Popa, the defendants argued that the plaintiff gave implied consent because the website contained a privacy policy.

The Third Circuit declined to address this defense because the district court had granted summary judgment on other grounds, which left the record on this question underdeveloped. As a result, the Popa decision leaves open the potential viability of this defense.

The potential success of this defense may depend, in the Third Circuit's estimation, on whether the privacy policy sufficiently alerts website visitors that their electronic communications are being sent to a third party.[11]

Even apart from the issue of consent, there are questions as to whether the data collected by this session replay code is actually the type of data collection covered by the statute, and if so, when the interception takes place, for resolving a jurisdictional challenge.

In Florida, which has a wiretap statute similar to Pennsylvania's, companies have had success arguing that the collection of browsing data does not fall within the scope of the Florida Security Communications Act, or FSCA.

Under the FSCA, which uses language identical to WESCA, an interception involves acquiring the contents of a communication, and "contents" is a defined term meaning the substance, purport, or meaning of that communication.[12]

In Goldstein v. Costco Wholesale Corp. in 2013 in the U.S. District Court for the Southern District of Florida, the court dismissed a claim under the FSCA based on browser tracking, stating the actions being tracked did not convey the substance of any communication but, rather, was analogous to the type of movement tracking that might be captured by a security camera at a brick-and-mortar store.[13]

Given the similarity in language between the Florida and Pennsylvania laws, a similar argument may be available for claims brought under WESCA.

Companies may also be able to assert jurisdictional challenges. Courts must necessarily determine where an interception occurred and whether there's a sufficient nexus to Pennsylvania to give its courts jurisdiction.

In Popa, the Third Circuit determined that the interception occurred when the plaintiff's browser, situated in Pennsylvania, delivered information that was routed to the defendants' servers out of state. While this may seem logical on its face, the picture becomes far more complicated given that individuals can access websites on their smartphones anywhere they want using mobile devices.

Not only does the use of mobile devices make it difficult to identify the point of interception

for jurisdictional purposes, it also raises constitutional concerns, such as implicating the dormant commerce clause.

Regardless of how the Third Circuit ultimately resolves these open questions, there are certain steps that companies can and should take to prepare for potential claims.

First, companies should ensure that their terms and conditions and privacy policies are conspicuously posted on their website.

Additionally, they should always closely review these policies to ensure that, to the degree applicable, they clearly state the manners in which visitors' information may be collected and aggregated by the company or third parties.

Second, in an effort to avoid potential arguments over whether a consumer impliedly consented to a privacy policy, companies can implement affirmative opt-in mechanisms that ask for consumers' express consent to the collection of information as described in a company's privacy policy.

These can take the form of banners or other pop-ups that ask website visitors to acknowledge and accept the privacy policy and agree to the use of tracking code or software. This will provide companies with additional evidence that all parties consented to the recording and that WESCA, therefore, should not apply.

Third, companies should review their agreements with third-party marketing vendors, website managers or other third parties who collect information from visitors of a company's website to determine whether those agreements provide indemnification related to this type of data collection.

Relatedly, companies should consider whether insurance is available to cover these types of claims.

The Popa decision represents a significant shift in applying WESCA. While defenses are available, many questions remain.

What is clear, however, is that Popa opened the door for a new batch of consumer class actions under WESCA, at least in Pennsylvania's federal courts.

Popa is binding on Pennsylvania's district courts until the Third Circuit states otherwise or until the Third Circuit certifies a question to the Supreme Court of Pennsylvania on the proper interpretation of the direct party exception.

Until then, companies should be careful to take the necessary precautions to prepare for potential future claims in this arena.

Thomas R. DeCesar is a partner and Jonathan R. Vaitl is an associate at K&L Gates LLP.

[1] Popa v. Harriett Carter Gifts, Inc., 45 F.4th 687 (3d Cir. 2022).

[2] 18 Pa.C.S. § 5701-5782

[3] 18 Pa.C.S. § 5703(1).

[4] See, e.g., Commonwealth v. Proetto, 771 A.2d 823 (Pa. Super. Ct. 2001); Commonwealth v. Cruttenden, 58 A.3d 95 (Pa. 2012).

[5] Specifically, the definition excludes direct communications to law enforcement "where the investigative or law enforcement officer poses as an actual person who is the intended recipient of the communication, provided that the Attorney General, a deputy attorney general designated in writing by the Attorney General, a district attorney or an assistant district attorney designated in writing by a district attorney of the county wherein the investigative or law enforcement officer is to receive or make the communication has reviewed the facts and is satisfied that the communication involves suspected criminal activities and has given prior approval for the communication." 18 Pa.C.S. § 5702.

[6] As of the time of this writing, the eleven cases have been filed across the three federal district courts in Pennsylvania. All of the cases bring claims against out-of-state defendants. The defendants include companies in various industries, but primarily target consumer retailers and online services companies.

[7] See, e.g., In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020).

[8] Cohen v. Casper Sleep Inc., 17-cv-9325, 2018 WL 3392877 (S.D.N.Y. July 12, 2018).

[9] 18 U.S.C. §§ 2510-2523.

[10] Cohen, 2018 WL 339287 at *3.

[11] Popa, 45 F.4th at 698.

[12] Fla. Stat. § 934.02(7); 18 Pa.C.S. § 5702.

[13] Goldstein v. Costco Wolesale Corp., 559 F. Supp. 3d 1318, 1321 (S.D. Fla. 2021).