PUBLICATION

Recent Wiretapping Class Action Dismissal Offers Compliance Lessons

Authors: David J. Oberly, Matthew George White, Aldo M. Leiva
April 08, 2025

In late March, an online retailer successfully asserted consent as a complete defense to a putative Pennsylvania Wiretapping and Electronic Surveillance Control Act of 1978 (WESCA)[1] class action lawsuit, resulting in the dispositive dismissal of the action. The decision provides key insights and lessons on how online notice and consent can be leveraged to directly address and mitigate legal risks and class action liability exposure arising from the use of cookies, pixels, and similar website tracking technologies and federal/state wiretapping statutes.

Implied Consent Bars Wiretapping Class Action Claims

In *Popa v. Harriet Carter Gifts, Inc.*, No. 19 CV 450, 2025 WL 896938 (W.D. Pa. Mar. 24, 2025), a website visitor filed suit against Harriet Carter Gifts, Inc. (Harriet Carter) and its technology vendor, NaviStone, Inc. (NaviStone), alleging that the companies unlawfully intercepted her data in violation of WESCA while she shopped on Harriet Carter's website. Harriet Carter's privacy policy, accessible through a hyperlink in the footer of its site, specifically disclosed both the collection and use of this website visitor data, as well as the access to that data by its third-party vendors.

Harriet Carter and NaviStone moved for summary judgment, arguing that the plaintiff's implied consent barred her WESCA claims as a matter of law. The court agreed, finding: (1) the privacy policy sufficiently disclosed the complained-of activities giving rise to the plaintiff's WESCA causes of action; (2) the privacy policy was reasonably conspicuous on the retailer's webpage so as to charge the plaintiff with constructive notice of its terms as a matter of law; and (3) through her continued use of the website, the plaintiff provided her implied consent to the retailer's data practices, including any "interception" that may have taken place on the site.

Like many all-party state wiretapping laws, WESCA bars the interception of electronic communications without the prior consent of all parties.[2] Pennsylvania's wiretapping statute also provides that *no* violation occurs "where all parties to the communication have given prior consent to such interception." An objective standard is used to determine the applicability of WESCA's consent defense to a given dispute, which looks to whether a "reasonably prudent person" can be deemed to have consented under the circumstances. Importantly, Pennsylvania courts have determined that the mere receipt of a disclosure providing notice that a website visitor's communications may be recorded may be sufficient; actual knowledge of the disclosure or its terms is not required.

Pennsylvania courts have utilized a two-part framework to evaluate whether consent bars WESCA causes of action. First, a privacy policy must sufficiently disclose the nature of the complained-of activities such that a reasonable person could have been apprised of such practices. Second, the privacy policy must be sufficiently conspicuous to put prudent users on inquiry notice of its terms. If both questions are answered in the affirmative, reasonable users are deemed to have provided implied consent through their continued actions on the site, and therefore, there is no WESCA violation.

Applying this framework in *Popa*, the court first determined that the terms of the retailer's privacy policy adequately disclosed the type of conduct that formed the basis of the plaintiff's WESCA claims. Specifically, the privacy policy alerted reasonably prudent website visitors of the "critical issue" for WESCA claims – that

third parties may collect, use, and otherwise have access to data concerning visitors' activities on the site. The court also determined that the privacy policy was presented on the site in a sufficiently conspicuous manner to place reasonably prudent users on inquiry notice of its terms and, in turn, visitors constructively consented to any "interception" of their data while on the site. Taken together, the court determined that the plaintiff could not establish an actionable WESCA claim as a matter of law, necessitating the dismissal of the action in its entirety with prejudice.

Notice and Consent Best Practices To Mitigate Wiretapping Class Action Risk

There are lessons to be learned from this case. In today's digital landscape, companies with an online presence face a growing wave of class action exposure tied to the routine use of cookies, pixels, and other common website tracking tools and technologies. Implementing strategic notice and consent measures – as part of comprehensive compliance programs – can directly address and mitigate these risks and associated liability exposure arising from the high volume of wiretapping class action filings that will only increase for the foreseeable future.

First, companies should ensure their privacy policies clearly and conspicuously disclose all online analytics, marketing, and tracking tools that operate on their websites and other online platforms. These disclosures should also encompass any related technologies or practices that may implicate the collection, use, or disclosure of visitors' personally identifiable information (PII), for example, any use of session replay technology or information collected through the use of video content. In *Popa*, the court highlighted several privacy policy provisions which, together, adequately informed visitors of the very practices that allegedly ran afoul of WESCA, including provisions explaining:

- the involvement of third-party vendors to support the retailer's online marketing and advertising campaigns;
- the use of cookies by the retailer and its vendors for purposes of collecting data concerning visitors' website activities and their interactions with the retailer's products and services;
- that no PII was collected during or through these activities; and
- that data collected from visitors during their use of the site may be combined with data obtained through other, outside sources.

Second, companies should ensure they present their privacy policies to website visitors in a clear and conspicuous manner that, at a minimum, puts them on inquiry or constructive notice of their terms.

There are two types of digital agreements commonly used for this purpose: clickwraps and browsewraps. Clickwraps, also referred to as click-through agreements, require users to expressly manifest their assent by clicking an "I agree" or similar button after being presented with a privacy policy link. Browsewraps do not require visitors to affirmatively manifest their assent, but instead ordinarily entail scenarios where a privacy policy is posted on a website via a hyperlink at the bottom of the site, there are no buttons to click, and users provide their assent simply through their continued use of the site.

Courts treat the enforceability of digital contracts on a spectrum, with clickwraps on one end and browsewraps on the other. Because clickwraps require affirmative action to manifest assent, courts regularly uphold their validity. In this respect, an electronic "click" generally suffices to signify assent to a privacy policy, so long as the layout and language of the site and clickwrap provide reasonable notice that the click will manifest assent. Because browsewraps do not require any affirmative action to be taken to manifest assent, many courts are more reluctant to uphold their validity. Accordingly, wherever feasible, companies should consider implementing clickwrap mechanisms while giving careful consideration to how they are presented to visitors. Importantly, companies using clickwrap need to test and ensure that none of their tracking technologies "fire" until users affirmatively manifest their consent.

How We Can Help

Given the widespread use of tracking technologies, these issues demand companies' attention. Today, many organizations deploy tools such as cookies and pixels on their websites – often without the broader business or legal teams being fully aware (usually only a few individuals in marketing know the extent to which these tools have been deployed). Companies should take proactive steps to understand their website's data practices rather than discovering them for the first time after receiving a demand letter or a complaint.

Moreover, as *Popa* indicates, the implementation of strategic notice and consent measures can significantly aid in addressing and mitigating the risk of being targeted with bet-the-company wiretapping class action litigation. Importantly, however – due to the myriads of nuances and potential pitfalls underlying notice and consent on the internet – companies should work closely with experienced outside privacy counsel who can assist in designing and implementing robust privacy disclosures and online consent mechanisms that maximize the likelihood of avoiding being named in a wiretapping class action complaint in the first instance. At the same time, appropriate measures will also arm companies with a complete liability defense in the event they find themselves targeted for purported noncompliance with federal or state wiretapping prohibitions.

Our deep bench of data protection, privacy, and cybersecurity specialists regularly counsel companies large and small on compliance and risk management strategies pertaining to WESCA, the California Invasion of Privacy Act (CIPA), and numerous other wiretapping statutes. We also frequently provide guidance to companies across all industries on a range of other website and online privacy matters, including the development of enforceable online clickwrap and browsewrap agreements. At the same time, our Data Protection, Privacy, and Cybersecurity team closely tracks and monitors new privacy and technology legislative, regulatory, and litigation developments, as well as emerging trends.

For more information or assistance with WESCA or wiretapping compliance or any related privacy or technology matters, please contact David Oberly, Matt White, Al Leiva, or another member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.

[1] WESCA is similar to other state wiretapping laws in that it regulates the interception and recording of communications – especially telephone and electronic communications – but, in fact, is notably stricter than many other state laws in a few ways. For these reasons, court decisions under WESCA can provide valuable guidance for interpreting other states' wiretapping laws.

[2] Alternatively, some states have single-party wiretapping laws (also called one-party consent laws) that allow a conversation to be lawfully recorded as long as at least one party involved in the conversation consents to the recording.