New Ruling on Social Media Tracking Reveals New Privacy Risks: What Your School Should Know About the Data It Collects

Insights
10.23.25

A recent privacy rights development could have major implications for any school or non-profit that has a website, as a Michigan federal court gave the greenlight for a video privacy protection lawsuit to proceed against nonprofit Hillsdale College over its use of webpage trackers. The October 17 decision is one of the first cases to apply the Video Privacy Protection Act (VPPA) in the context of website tracking software. Allowing the lawsuit to advance under the VPPA past the pleading stage opens the arena for similar privacy claims to be brought under federal law and exposes businesses – including schools and non-profits – to potential lawsuits nationwide. Here's how you can stay ahead.

Setting the Landscape

While most privacy and surveillance-based litigation has been brought under state laws, US District Judge Hala Jarbou in the Western District of Michigan determined that Hillsdale College was subject to the federal VPPA when it allegedly shared certain information with a third-party social media company, including the viewing histories and social media account IDs of individuals who viewed educational videos on Hillsdale's website.

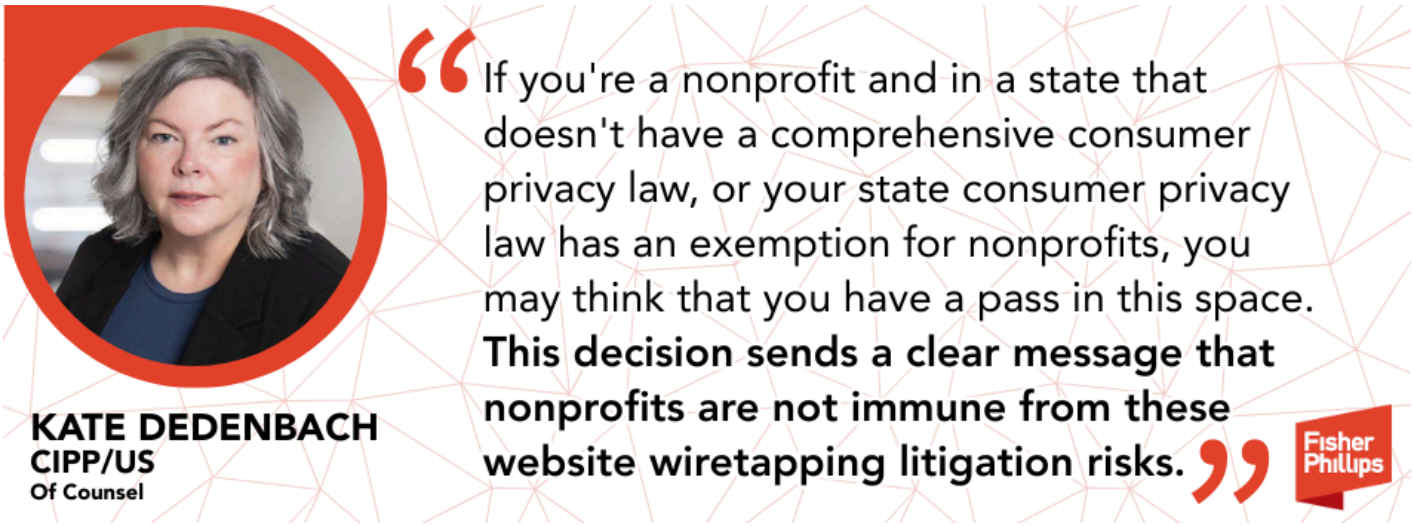
The VPPA protects video viewing history and includes a private right of action against "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider."

The plaintiffs in the case allege that Hillsdale College's use of a pixel tracker to share information about individuals who viewed educational videos on the school's website, including their social media account IDs, violated the VPPA.

The district court's broad interpretation that social network account IDs are considered personally identifiable information presents new risks for any entities that have integrated social media into their online presence.

The decision lands amid a growing trend of wiretapping and consumer privacy cases being filed across the country alleging that a business or non-profit's use of third-party website tracking technology – including cookies, chatbots, analytics tools, software development kits (SDKs), and other website software – violates state law. For example, litigation brought under statutes in

Florida and California have seen some success, though a recent ruling under California law in favor of a website operator is promising. Moreover, Massachusetts has shut down similar claims brought under its wiretapping law.



Does My School or Nonprofit Have to Comply With This Law?

The Michigan federal court decision sets out an expansive reading of who is a "video tape service provider" that is subject to the VPPA.

Although a number of state consumer privacy laws include exemptions for nonprofits, they aren't immune from liability under the VPPA. District Judge Jarbou reasoned that Hillsdale College would be "engaged in the business of" delivering videos regardless of whether the video delivery produces revenue or turns a profit.

"If you're a nonprofit and in a state that doesn't have a comprehensive consumer privacy law, or your state consumer privacy law has an exemption for nonprofits, you may think that you have a pass in this space," said Kate Dedenbach, Of Counsel in Fisher Phillips' Detroit office. "This decision sends a clear message that nonprofits are not immune from these website wiretapping litigation risks."

What Information Counts?

Courts have ruled differently on what it means for information to be "personally identifiable information" (PII).

The VPPA defines such information as data "which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

The 2nd, 3rd, and 9th US Circuit Courts of Appeals use an "ordinary person" standard to determine if information is PII, which weighs whether the information would allow an "ordinary person" to identify a specific person's video-watching.

Under this analysis, the Western District of Michigan found that URL and social network account ID information constituted PII because an ordinary person could use the ID to discover someone's identity. The judge also reviewed the college's disclosures under a broader lens, finding that if the recipient of the data disclosure can use it to determine an individual's identity, the information is considered PII.

The court's reading that a social media user's account ID is PII could have major impacts for businesses who use social media plug-ins, even if they don't have videos on their website.

"This should be a concern for any entity that's using social media IDs and sharing them," said Dedenbach.

And while the VPPA only applies in the case of videos, Dedenbach says that the court's analysis of what constitutes PII – particularly its determination that URL and social network account IDs count as PII – could be applied to other non-video type privacy claims.

How Can I Protect My School Website?

- **Provide Notices:** Schools and nonprofits that want to share user data for marketing or analytics purposes should consider banners or other notices to ensure they have consent to disclose the information.
- **Consider Additional Measures:** You can also configure your websites to ensure that no data is shared with third parties until you receive consent from a visitor.
- **Conduct a Compliance Audit:** You should also consider conducting a comprehensive review of your websites to ensure you are aware of what data is being collected and shared.
- **Track Litigation Trends:** Fisher Phillips has a dedicated team of attorneys working on this every day, and we have created a Digital Wiretapping Litigation resource page with articles and updates to help businesses and nonprofits avoid being the subject of this new wave of litigation.

Conclusion

The ruling from the Western District of Michigan could be appealed, but it serves as a good reminder to review your data collection practices and disclosures, given the rapidly evolving case law in this space. We 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. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group, Consumer Privacy Team, or Education Team.

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Data Protection and Cybersecurity

Digital Wiretapping Litigation

Industry Focus

K-12 Institutions

Education

Higher Education

Trending

U.S. Privacy Hub

Related Offices

Detroit