Insights, News & Events

3RD CIRCUIT OFFERS CLARITY ON DATA PRIVACY AND REPLAY CODE: 3 PROACTIVE STEPS FOR YOUR BUSINESS FOLLOWING DUAL RULINGS

Insights
Jun 5, 2026

3rd Circuit Offers Clarity on Data Privacy and Replay Code: 3 Proactive Steps for Your Business Following Dual Rulings

Over the last few years, the plaintiffs' bar has frequently cited businesses' use of session replay code (SRC) on websites as one basis for the flood of website tracking litigation against businesses across the country. SRCs allow domain hosts to track nearly every element of a website visitor's activity – from mouse movements to clicks, scrolls, zooms, and keystrokes – allowing the host to effectively recreate the user's visit to their website. Since SRCs typically operate without a visitor's consent, a wave of class action lawsuits has been filed alleging that SRCs effectively constitute digital wiretapping since they intercept and log behavior in real time. Although there have been mixed decisions across the country on motions to dismiss such claims, a pair of recent decisions from the 3rd Circuit Court of Appeals provides important guidance that can help businesses to avoid and defeat such claims. This Insight will cover everything you need to know about the rulings and what you can take away for your business.

Data Disclosure Doesn't Always Amount to a Tort

Plaintiffs in both cases before the 3rd Circuit alleged that businesses using SRC on their websites violated the common-law torts of disclosure of private information and intrusion upon seclusion. But the court tossed the cases,

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner

610.230.2132

Logan S. Booth, CIPP/US
Of Counsel

finding that the plaintiffs failed to show any injury from the technology and lacked standing to sue.

In one case against a defunct budget airline, the court ruled that the tort of disclosure of private information was not applicable because the information collected by the SRC was not used to **embarrass or humiliate** the plaintiffs – a **necessary element** of such claim. The judges also held that the airline did not commit intrusion upon seclusion because (i) the plaintiffs voluntarily provided the information to the SRC, (ii) their information was anonymized, and (iii) there is a limited expectation of privacy on the Internet.

Similarly, in another case involving outdoor retailers, the court determined that "mouse clicks and movements, keystrokes, and search terms" didn't amount to sensitive information and couldn't be linked to the plaintiffs' identities. Thus, the plaintiffs in this case couldn't plausibly allege that disclosing this information caused "**embarrassment or humiliation.**"

In this case, however, the 3rd Circuit went a step further and clarified that the mere collection of sensitive financial information – without subsequent revelation – fails to meet the threshold needed to prove disclosure of private information.

For individuals who merely perused the retailers' websites without inputting any personal information, the court held that their activity on the website generated no greater expectation of privacy than a shopper would have while walking the aisles of a brick-and-mortar store. Nevertheless, once a visitor to the website entered their complete credit or debit card numbers, the recording of that information by the SRC **did qualify** as an intrusion upon seclusion, since the sensitivity of financial information makes any nonconsensual interception particularly harmful.

What's the Impact of This Ruling?

It's important to keep in mind that the 3rd Circuit's decision is only binding on the states within its jurisdiction, which include **Delaware**, **New Jersey**, **Pennsylvania**, and the **US Virgin Islands**. But, within this circuit, the Court has shown consistency in ruling against plaintiffs in related wiretapping and privacy disputes. For example, in *Popa v. Harriet Carter Gifts, Inc.*, the Court held that simply browsing an online

720.644.2889

Catherine M. Contino

Associate

610.230.6109

Service Focus

Data Protection and Cybersecurity

Litigation and Trials

Privacy and Cyber

retailer's website without entering sensitive information failed to rise to the level of an injury-in-fact.

And for those outside the jurisdictional purview of the 3rd Circuit, these holdings can be used by other courts as persuasive authorities. The 9th Circuit has already issued a similar ruling in *Popa v. Microsoft Corporation*, in which it held that the routine use of web-analytics and session-replay tools does not run afoul of wiretapping laws or yield "concrete" harm. Whether other courts borrow of these precedents, and how the Supreme Court ultimately rules if it takes up a case addressing these issues, will be important considerations for how website operators should conduct themselves moving forward.

What This May Mean for Your Business

The 3rd Circuit's rulings that the mere recording of a user's activity on a company's website, absent additional factors, does not automatically constitute digital wiretapping is a major win for domain hosts. It provides hosts with the ability to control the liability they may face from employing SRCs based on what type of information they gather and how that information is used. Following this ruling, you should work with legal counsel and consider reviewing:

- **What type of information is your SRC collecting?**

It's important to audit and frequently review the types of information collected by your SRC. Merely recording a user's "movements" on your platform likely will not give rise to a tortious claim. Even if a consumer is accessing your websites from the confines of their home, the 3rd Circuit is inclined to view their activity on your website like a shopper moving through a physical store. In the same way that the physical shopper has no expectation of privacy vis-à-vis their movements, the website visitor should not, either.

- **Would a reasonable person consider the information gathered by your SRC to be highly sensitive?**

While mere movement within a web domain is not inherently sensitive, the collection of **financial information** is. This means that before a user inputs financial data, one of two things must occur: the website (i) must obtain consent to continue utilizing SRCs or (ii) terminate the use of SRCs if the user is not given the choice to opt-in to the collection of this information. The same is likely true of other categories

of sensitive personal data, including health-related information.

- **How can you design an SRC-compliant website from the outset?**

In its decisions, the 3rd Circuit specifically called out the "surreptitious" nature of SRCs, and the fact that websites often do not give users the option to opt-out, nor does the average user even know that SRCs are embedded in the websites they visit. It is this element of secrecy that creates potential legal liability for website operators. As such, in the same way that cookie banners have come to be viewed as a means of limiting exposure for tracking a user's Internet activity, it may be prudent for companies using SRCs on their website to consider deploying similar disclosure notices.

Conclusion

Fisher Phillips will continue to monitor developments 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 Data Protection and Cybersecurity Practice Group.