Brown & Brown

PROPERTY & CASUALTY

Web Tracking and Pixels

Julia Krzeminski, Miles Crawford, Christopher Keegan, and Britt Eilhardt

Website tracking technologies have become the center of attention in privacy litigation, as the plaintiffs' bar capitalizes on various privacy statutes and tort laws to file class actions, which have often resulted in significant multi-million-dollar settlements. In this two-part series, we explain:

- **Part 1:** Pixel tracking overview, related statutes and regulations and how they can be leveraged against companies.
- **Part 2:** Settlement value of cases, compliance considerations and potential implications for your cyber coverage.

What Is Pixel Tracking

Pixel tracking is a tactic widely used in advertising and analytics to measure user interactions and monitor online behavior to collect valuable consumer data. It is one of several types of website tracking that companies utilize (e.g., pixels, chatbots, session replay and video tracking). Tracking pixels can provide insight into email opens, page views, impressions, website clicks, sales conversions and other information that gives insight into users' online activity. Unlike cookies, tracking pixels are not dependent on a browser for functionality and can operate independently to send information directly to web servers. Tracking pixels can provide more data than cookies because they have the ability to follow users across devices and cannot be easily disabled.

Meta Pixels are a retargeting pixel that tracks user activity through cookies to collect data on HTTP headers, button click metrics and user-specific data that is then shared directly with Meta. This data can then be used to create targeted campaigns and deliver personalized messaging. Meta Pixels have become the focus of data privacy litigation, resulting in at least one hundred class-action lawsuits in the past year. In addition to federal and state data privacy regulations, lawsuits allege intrusion upon seclusion, negligent misrepresentation, invasion of privacy, breach of contract, breach of fiduciary duty and more as causes of action.

Privacy Regulations and Litigation

The plaintiffs' bar relies on several privacy statutes to limit the tracking of individuals' activity on websites, regardless of the company's industry. However, there is sensitivity and settlement value in healthcare, which is where these suits originated.

Health Insurance Portability and Accountability Act (HIPAA)

Numerous legal observers have noted that more than 50 class-action lawsuits were filed against hospitals and healthcare systems for HIPAA-related violations associated with pixel tracking in 2022 alone.[1] When a regulated business or entity subject to HIPAA uses pixel tracking technologies developed by a third party on their mobile app or website, such use may result in the collection and/or disclosure of personal health information to the third party. An investigation of healthcare and hospital websites found that 33 out of 100 hospitals in the United States use Meta Pixels on their websites.

Adding to existing concerns in the healthcare space, in December 2022, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services issued a bulletin to give guidance on pixel tracking[2]. The bulletin stated that regulated entities are prohibited from utilizing tracking technologies in a way that would lead to unauthorized disclosures of protected health information to tracking vendors or any other violations of HIPAA rules. The OCR further defined tracking technologies as a script or code on a website or mobile app used to gather information about users as they interact with the website or app (including cookies, tracking pixels, chat functions and any other tool that discloses information about the user to a third party).

Entities subject to HIPAA should conduct an audit of any tracking technologies used on their websites, web applications or mobile apps to determine if they are being used in a manner that complies with HIPAA. If it is discovered that the past or ongoing use of these technologies violates HIPAA, consumer notification may be required.

Video Privacy Protection Act (VPPA)

In addition to HIPAA, the 1988 Video Privacy Protection Act, which forbids sharing audiovisual media usage data, has become a prominent subject in recent privacy litigation. Initially implemented to regulate the sharing of rental history and information by video tape service providers during the era of Blockbuster and video tapes, the rise of pixel tracking and online streaming has brought about a resurgence of VPPA-related litigation.

Since February 2022, no fewer than 47 proposed class-action lawsuits have been filed against retail, news outlets, streaming services and sports organizations citing VPPA-related violations. The merits and viability of VPPA litigation are strong, demonstrated by a 2022 lawsuit against Boston Globe Media Partners LLC, settling for five million dollars after the judge denied the defendant's motion to dismiss. While not every lawsuit will be successful due to company arbitration or class waiver clauses, VPPA litigation is forecasted to increase in the coming years until companies adapt or forego the use of pixel tracking.

Wire Fraud and Other Statutes

Creative litigants have resurrected federal and state wiretapping statutes and more traditional privacy causes of action – intrusions upon seclusion, breach of contract, invasion of privacy, etc. – to pursue data-tracking cases. Many companies have been using data-tracking technology for years. While some wiretapping acts allow recovery of statutory damages ranging from $1,000 to $25,000 per violation, recent innovations by law firms have opened the possibility of large judgments and settlements.

---

[1] *McKeon, J. (2023, April 27). Data Breach Lawsuits Tied to Tracking Pixel Use On the Rise In Healthcare. HealthITSecurity.* https://healthitsecurity.com/news/data-breach-lawsuits-tied-to-tracking-pixel-use-on-the-rise-in-healthcare.

[2] *U.S. Department of Health and Human Services (2022), Use of online tracking technologies by HIPAA covered entities and business associates. HHS.gov.* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

The most significant driver of the valuation of these cases is the prospect of class certification. It remains to be seen whether plaintiffs will be able to sidestep the traditional common law and class certification defenses with claims for statutory damages under state laws. Although healthcare, consumer and retail companies are currently in the spotlight, any company that tracks data on websites could become a target and should be paying attention to the risk.

Implications for Cyber Coverage

The prevalence of class-action lawsuits related to web tracking technologies emphasizes the importance of comprehensive cyber coverage. Insureds should consider the following basic steps when selecting cyber insurance:

- **Coverage Evaluation:** Review existing cyber insurance policies to determine if coverage encompasses potential liabilities from user tracking practices. Assess whether the policy includes coverage for privacy violations, data breaches, regulatory fines and class-action lawsuits related to tracking technologies.
- **Risk Assessment:** Conduct a thorough risk assessment to identify vulnerabilities and potential exposures associated with user tracking. This assessment should consider the type and extent of tracking technologies employed and their compliance with privacy regulations.
- **Policy Limits and Deductibles:** Evaluate policy limits and deductibles to ensure they align with potential liabilities arising from class action lawsuits. Adequate coverage should be in place to mitigate the financial impact of settlements or judgments.
- **Legal and Regulatory Updates:** Stay informed about changes in privacy laws and regulations to ensure cyber insurance coverage remains up-to-date and compliant with evolving legal requirements.
- **Incident Response Preparedness:** Develop and regularly update an incident response plan with specific provisions for privacy-related incidents and class-action lawsuits. This plan should outline steps to be taken in a lawsuit, including engaging legal counsel, notifying insurers, and coordinating with public relations and crisis management teams.

By adopting these recommendations and securing cyber insurance coverage, insureds can enhance their preparedness to help mitigate risks associated with user tracking technologies and other emergent cyber risks.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com