Brown & Brown

PROPERTY & CASUALTY

Evolving Privacy Exposures - Web Tracking Pixels

Julia Krzeminski, Miles Crawford, Christopher Keegan and Britt Eilhardt

In our first article Web Tracking and Pixels we discussed Pixel tracking overview, related statutes and regulations and how they can be leveraged against companies. Read more here https://www.bbrown.com/insight/web-tracking-and-pixels/

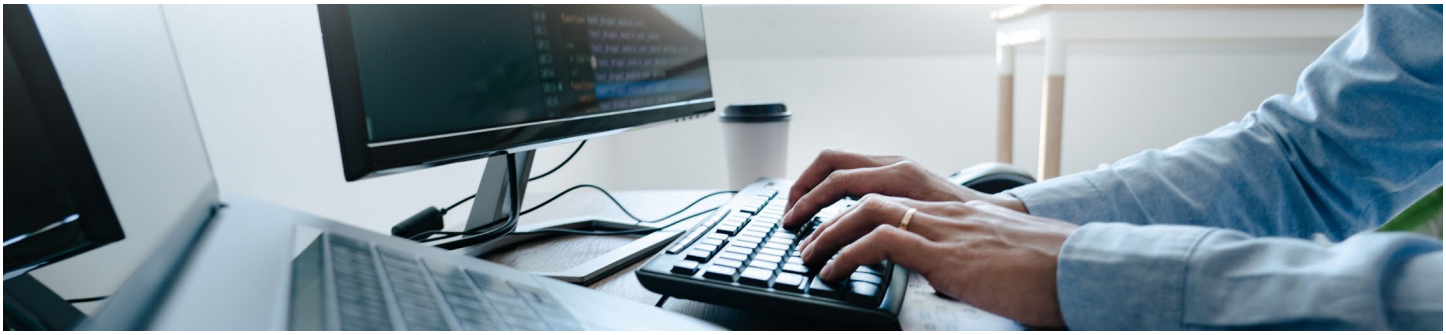
Over the past several years, a wave of legal action has been filed against organizations that employ web tracking technologies on their platforms. These class action lawsuits differ from typical data breach litigation, focusing on privacy concerns and data access rights rather than security. Many of these suits have arisen because the plaintiffs allege that the data collected is shared without proper notification or consent. The specific technologies under scrutiny in these lawsuits are those similar to and include Meta Pixel tracking, which records and shares certain consumer information regarding their activities on websites. Notable examples and categories of these suits include the following:

Meta Pixel Tracking and Class Actions Against Healthcare Providers

Numerous cases have been filed against healthcare providers who deployed Meta Pixels on their websites. Plaintiffs have had mixed success, as it is difficult to prove the nature of the data shared with Meta. For instance, one case filed in California in 2016 was dismissed because the plaintiffs could not provide evidence that Facebook had gathered protected health information according to HIPAA's definition. More recently; however, healthcare providers have faced more demanding challenges. In 2019, Massachusetts General Brigham Health settled by paying $18.4 million to their plaintiffs due to allegations of data sharing with Meta.

Oracle and Salesforce Cookie Tracking Class Action

In 2020, Oracle and Salesforce faced class-action lawsuits in the U.K. and the Netherlands over using third-party cookies for ad tracking and targeting. The pending lawsuits argue that mass surveillance of internet users for real-time auctions of marketing data violated the GDPR. The litigants alleged that Oracle and Salesforce breached the GDPR by processing and sharing people's information via third-party tracking cookies and other advertising technology methods without informed and specific consent. The collective claims were assessed to exceed 10 billion euros.



Meta Pixel Tracking and Class Actions Against Media Companies

In 2022, more than 50 class-action suits were filed against media companies that deployed Meta Pixel on their platforms. These suits alleged that the media companies, including ESPN, Bloomberg, NPR and the NFL, used Meta Pixel Tracking technology, which shared user's behavioral data back to Meta. These suits are based on alleged violations of the Video Privacy Protection Act (VPPA), which forbids sharing audiovisual media usage data. As of mid-2023, many defendants requested the suits go to arbitration. Some defendants have had success asserting the information shared was aggregated and anonymized, meaning it would be impossible to identify a particular user's information based on the data shared with Meta.

Meta Pixel-Based Class Actions against Financial and Tax Services Providers

Several popular tax-filing websites utilized Meta Pixel Tracking to transmit sensitive financial information to Meta, enabling the social media giant to collect visitor data. Major tax preparation services, like H&R Block, TaxAct and TaxSlayer, were alleged to have sent users' income, filing status, refund amounts and dependents' college scholarship amounts to Meta through their tracking pixels. Several class actions have been filed and are being carried out in the courts.

Other Web Tracking Technologies

Web tracking technologies are an integral part of the modern digital landscape. They shape how users interact with online content, delivering personalized experiences and providing feedback to service providers. Pixel Tracking is just one of these technologies. From the early days of cookies to the emergence of sophisticated tracking mechanisms like device fingerprinting, the evolution of web tracking has long sparked debates about user privacy and data security.

Cookies

Web Cookies, or HTTP cookies or browser cookies, are small text files stored on a user's device by websites they visit. They can store user preferences, track browsing behavior and provide personalized experiences. Cookies have been around since the earliest days of the internet and have been indispensable in supporting the functionality of web pages ever since. Although initially designed to facilitate the storage of a user's site preferences, Cookies rapidly grew popular as a data tracking and advertising tool. In 2009, the European Union introduced the "EU ePrivacy Directive," which required websites operating within the EU to obtain informed consent from users before storing or accessing cookies on their devices. The concerns echo the trajectory of the EU Cookie Directive and push to regulate Pixel Tracking today.

JavaScript Tracking

JavaScript tracking has been a widespread practice in web development for many years, allowing website owners and third-party advertisers to collect various data about users' interactions and behavior on websites. JavaScript was introduced in 1995 by Netscape. Initially, JavaScript was primarily used for client-side interactivity, enabling developers to create dynamic and interactive web pages. As the web evolved, developers started leveraging JavaScript for various purposes, including tracking user behavior. Further developments in the early 2000s expanded the capabilities of JavaScript, making it easier to send and receive data from web servers in the background, which allows developers and marketers to track user interactions more seamlessly. Similar to web cookies, JavaScript can gather extensive information about users, such as browsing history, mouse movements, clicks and form submissions, potentially infringing on user

privacy. JavaScript tracking could be utilized to track users across different websites, creating profiles of their online activities without explicit consent.

Device Fingerprinting

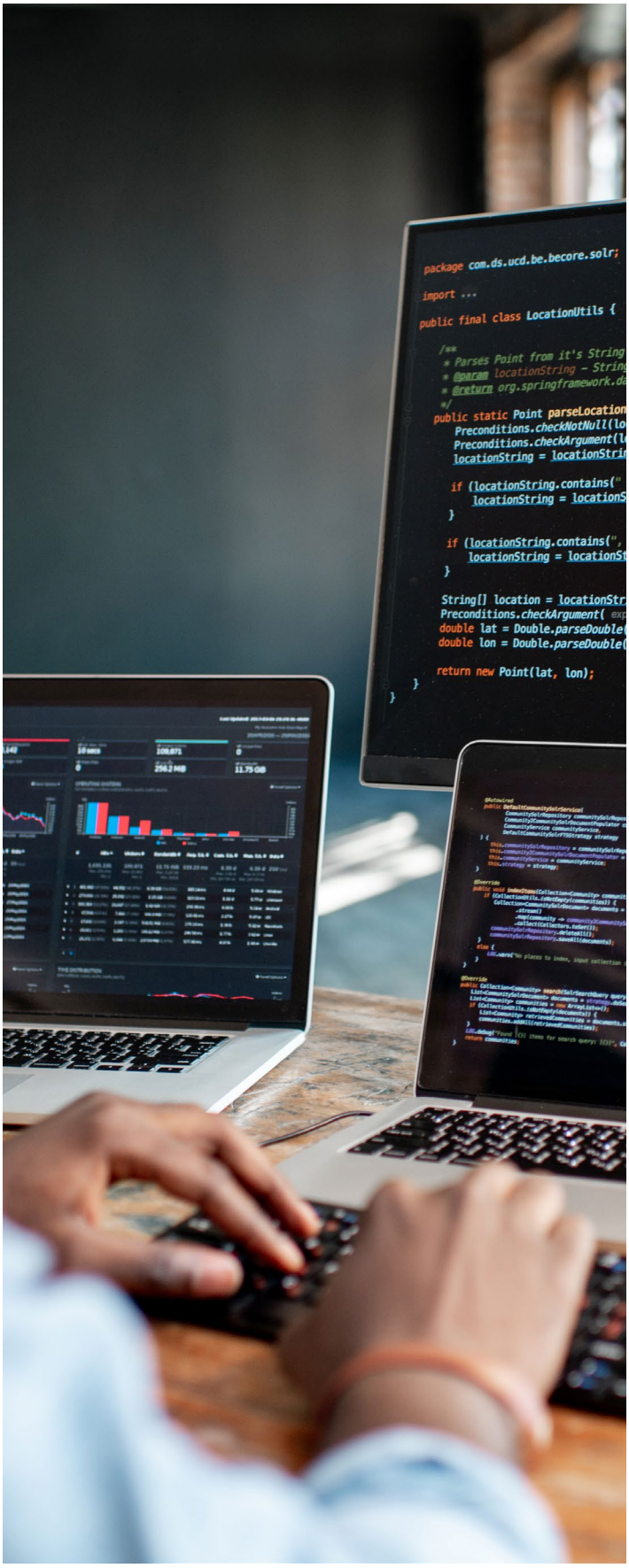
Device fingerprinting employs a technology that collects information about a user's device, including its operating system, browser version, screen resolution and installed plugins. By combining these attributes, a unique identifier can be created to track users across different websites. The concept of device fingerprinting dates to the early 2000s, with the increasing need to track and identify devices even when traditional tracking methods like cookies were blocked or deleted. Today, tracking pixels can be used as a supporting technology for device fingerprinting. Device fingerprinting gained popularity as a fraud detection and prevention tool, providing an additional layer of security for online transactions. Over time, device fingerprinting evolved, and its use expanded beyond fraud prevention. Advertisers, analytics companies and data brokers started using device fingerprinting to track users across devices and browsers, creating comprehensive profiles of their online activities and behaviors.

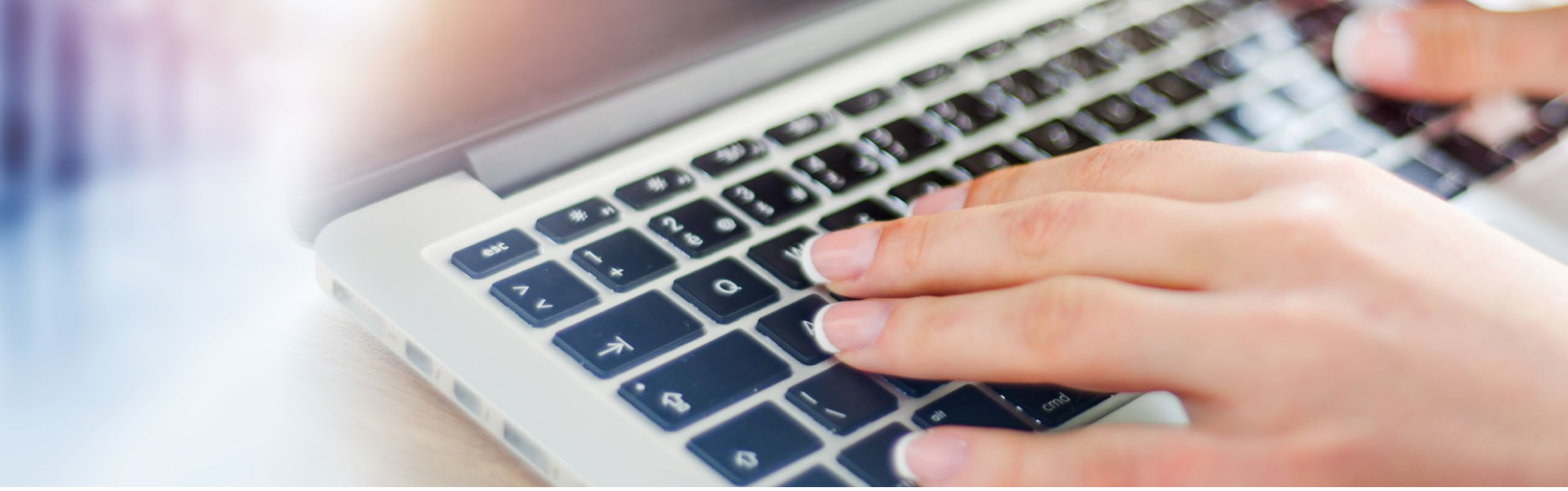
Ad Networks and Behavioral Advertising

Ad networks, particularly those engaged in behavioral advertising, have raised concerns about data privacy. These networks can employ multiple tools, including machine learning and pixel tracking, to collect large volumes of user data to display targeted ads based on users' online behavior. These practices have led to concerns about user profiling and data misuse. Google, Salesforce and Oracle have large ecosystems of marketing services that have received criticism for their lack of transparency and extensive reach.

Session Replay

Session Replay is a technique designed to capture user interactions on a website by recording information at regular intervals. It involves creating a detailed recreation of a user's interface, pixel by pixel, allowing web hosts to "watch" a video-like playback of a user's engagement with the site. Recording can be facilitated using various web technologies and usually encompasses various actions like mouse clicks, keyboard inputs, cursor movements and zooming. The recorded data can be presented in aggregated forms, such





as heatmaps, providing insights into overall user behavior or, individually, offering the ability to review a particular user's experience. The primary goals of session replay include enhancing consumer experience, ensuring compliance and optimizing website functionality.

Recommendations and Best Practices

New technologies and regulations around data privacy are reshaping consumer expectations about how organizations should use data and tracking technologies. While many organizations recognize the importance of data responsibility, maintaining adherence to these principles is challenging, given the rate of change. To minimize risks, insureds should consider the following recommendations:

- **Data Minimization:** Minimize the collection and retention of personal data to only what is necessary for legitimate business purposes. Avoid collecting sensitive personal information unless explicit consent is obtained and a lawful basis for processing exists.
- **Data Aggregation:** If user behavior data must be collected, it is best practice to aggregate and anonymize this data. Aggregation can address privacy concerns, but it also diminishes the usefulness of mobility data for applications that demand more detailed and specific information.
- **Internal Coordination:** Organizations should internally coordinate across all teams to effectively balance business objectives and potential risks. Collaborative efforts enable organizations to find solutions that minimize the likelihood of privacy breaches, liability and regulatory non-compliance while maximizing the effectiveness of their technologies.
- **Security Measures:** Implement robust security measures to help protect collected data from unauthorized access, breaches and cyber threats. Regularly assess and update security protocols to stay ahead of emerging risks.
- **Third-Party Vendors:** Conduct due diligence on third-party vendors or service providers who handle user data on your behalf. Ensure that these vendors adhere to privacy regulations and have appropriate data protection measures in place. Seek contractual indemnifications for failures to appropriately protect sensitive information.
- **Data Subject Rights:** Respect users' rights, such as the right to access, rectify, erase and restrict the processing of their personal data. Establish procedures for handling user requests related to data subject rights.
- **Transparency and Consent:** Implement transparent practices regarding user tracking. Clearly communicate to users the types of tracking technologies employed, the purpose of data collection and obtain their informed consent. Provide accessible and easily understandable privacy policies and cookie consent mechanisms.
- **Regular Reviews of Data Practices:** Ensure legal, marketing and other equity holders confirm the disclosures, consents and privacy policy contents to ensure they align with the types of datab collected and the usage of that data. Stay informed and comply with relevant privacy regulations, such as the GDPR, CCPA, BIPA and other applicable laws.

By adopting these recommendations and securing appropriate cyber insurance coverage, insureds can enhance their preparedness to 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