"Pixels" and "Cookies," Charming Terms for Tracking Technology, Can Lead to Ugly Data Privacy Headaches

Molly Arranz and **Sofia Valdivia** Amundsen Davis LLC

Companies in all industries and of all sizes are evaluating sophisticated and useful technology for their websites and applications (their "apps") in an effort to enhance and develop their image or brand and to support the marketing and sales of products or service offerings. Chief among them are tracking technologies, such as pixels and cookies, code that can be embedded in a company's website, for instance. Historically, this tracking technology has been considered to collect de-identified data points about user behavior, such as where a person "clicks" on the website, what searches are being performed, and what kind of "traffic" certain offerings on the website get.

However, caution should be exercised when using these tools—advancing at a lightning pace—because they sit at the heart of an emerging area of data privacy litigation.

SOME BACKGROUND

When you visit a company website, it is now commonplace to see a "cookie pop-up" asking you what kinds of cookies you will accept during your visit. There are lesser-known kinds of tracking technology offerings, such as pixels, that can be running on a company's website as well. Tracking pixels are code snippets embedded on a website, which are nearly invisible on the website but contain a "tag" that tracks user behavior.

Is this tracking technology capturing website visitors' names, addresses, emails, phone numbers or any sort of traditional "personally identifiable information?" No. Instead, the substantive data points captured, recorded and potentially shared with third parties are mouse clicks, navigation through webpages, time spent on certain webpages, and perhaps searches conducted on a webpage. And, yet, these seemingly anonymized and de-identified activities in combination with antiquated statutes, such as the federal Wiretapping Act, have fueled privacy class action litigation as of late.

Companies should remain vigilant as to how advancements in technology and software applications intersect with the potential consent and disclosure requirements of older statutes and current privacy regulations because, otherwise, businesses

may find themselves unwittingly subject to this emerging area of data privacy and consumer privacy litigation.

SESSION REPLAY TOOLS

Take, for instance, a tracking technology known as "session replay." This technology offering can help a company review and then analyze what website visitors do when they navigate across webpages. Session replay tools visually recreate user moves and mouse clicks, providing valuable insight to multiple teams across a company's organization. This helpful and seemingly-privacy-neutral technology has prompted allegations, in recent consumer class actions, that companies using this technology are illegally wiretapping visitors to the website.

Plaintiffs claim that session replay tools are improperly "recording their interactions" on a company's website without the requisite consent. Notably, the states where these cases are pending are each "all-party consent" states, meaning that explicit consent is required from both parties prior to "recording" communications and interactions. This is why consumers are made aware of phone calls being on a recorded line when a company is contacted for customer support, for example. Now, through creative pleading, consumers are alleging a failure to obtain this same consent for the "monitoring" or "recording" via this tracking technology.

Notably, as of this summer, federal district court judges in Delaware and Florida have dismissed these session replay lawsuits. A Delaware federal court found that there was no injury or invasion of privacy because the sessions were only tracking consumer behavior. There was no injury, in fact, if plaintiffs cannot claim that companies are obtaining personal information or attempting to monetize the information collected. However, plaintiffs have also had some recent wins. Last year, the Third Circuit found that the transfer of consumer data from a business's website to its service providers, through session replay tools, was an "interception" under Pennsylvania's state wiretapping law. And the Ninth Circuit held that businesses must obtain prior express consent from users for their use of session replay software under the California Invasion of Privacy Act. Of course, as many of the lawsuits concerning data privacy are still pending, the opinions in this area of law are still developing.

TRACKING PIXELS IN THE HEALTH CARE INDUSTRY

Tracking pixels, such as those offered by Meta (Facebook) and used in Google Analytics, have also been under fire recently. Like session replay tools, these pixels track user behavior, site conversions, web traffic, and other metrics. This information can help businesses deliver a better website user experience, showcase relevant advertisements, and identify unnecessary costs in marketing campaigns. While the use of these pixels is not new, the litigation surrounding them is, and healthcare providers and health-related entities that use these pixels may find themselves litigating on a new front.

Specifically, consumer privacy class actions, filed in both federal and state courts, contain claims that healthcare entities that use tracking pixels to analyze page clicks and other consumer behaviors are collecting and disclosing personal health information (PHI) to third parties like Google and Meta. Plaintiffs are attempting to push the bounds of the historic understanding of covered entities' disclosures of PHI. Like the session replay litigation, in these lawsuits, plaintiffs claim violations of federal and state wiretapping laws, invasion of privacy, and breach of certain duties, amongst other claims. While the health care industry is the current target for tracking pixel allegations, the breadth of this litigation may be expanding. Just this past summer, retailers, companies in the finance industry, and entertainment providers have faced lawsuits regarding their use of tracking technologies.

WHAT THIS MEANS FOR YOUR BUSINESS

The vast uncertainty around the merit to these consumer claims based upon tracking technology translates into the very real chance of future class action lawsuits based on these purported "invasions of privacy." This also means the extent of exposure is unknown; it may be significant, especially since the federal Wiretap Act has a substantial statutory amount recoverable for violations. These lawsuits should prompt you to gain a deeper understanding about the tracking technology you use and what is provided by your third-party service providers. Specifically:

1. **Have regular discussions with your marketing team on what tools they are using to measure consumer engagement.** A great team will continue to take advantage of new technology and analytic tools to grow your business. But as technology continues to advance, so does the legal landscape surrounding this technology. It is important to have ongoing discussions with your various internal teams to ensure that you are aware of not only what tools they are using, but how, in order to assess which outward-facing disclosures need to be made.

2. **Routinely assess how your company collects and uses the data it collects.** What often makes data privacy tricky to navigate is that there is no one size fits all approach when it comes to compliance efforts. Your obligations for disclosures to website visitors, consumers and even your business partners will depend on a variety of factors, including from where the data is coming, how it is being collected, and what is being collected. And, as recent privacy class action lawsuits have taught us, the laws and legal recommendations are only continuing to emerge and evolve. Businesses need to have a comprehensive understanding of what data they actually take-in or collect and how it is being used in order to ensure proper consent gathering and privacy disclosures.

3. **Evaluate other data privacy "risks" - i.e. your data security structure and practices.** These lawsuits are brought against a backdrop of growing concern over whether companies are appropriately analyzing, identifying and minimizing their data privacy risks. While you evaluate the consumer consent gathering and disclosures on the front-end, take time to review and audit your compliance with your cybersecurity and data protection obligations. Now is the time to update and likely upgrade your internal policies, practices and training for data collection, protection and sharing.

Molly Arranz is the chair of Amundsen Davis's Cybersecurity & Data Privacy Service Group and a partner in the firm's Chicago office. Contact: marranz@amundsendavislaw.com

Sofia Valdivia is an associate in Amundsen Davis's Cybersecurity & Data Privacy Service Group. Contact: svaldivia@amundsendavislaw.com