Another Data Collection Tool Leads to Privacy Class Actions

Article
Amundsen Davis Cybersecurity & Data Privacy Alert
March 9, 2023

As companies look to innovative and useful technology to enhance their brand development and the marketing and sales of products or services, they need to remain cautious of how these tools—advancing at a lightning pace—intersect with (often, antiquated) statutes and regulations.

Take for instance: a tracking tool, known as "session replay," which can help a company review and then analyze what website visitors do when they navigate webpages. Session replay tools visually recreate moves and mouse clicks, providing valuable insight to multiple teams across a company's organization including web developers, product developers, and marketers. And, yet, this helpful and seemingly-privacy-neutral technology sits at the cornerstone of some of the latest consumer class actions, where consumers allege that the companies using this technology are illegally wiretapping them. Like many other data privacy class actions, no data points traditionally viewed as "personally identifiable information" are collected.

Plaintiffs claim that session replay tools are improperly recording their interactions on a company's website without the requisite consent. Yet again, the question of permission or consent comes into play in the data privacy landscape. The more recent cases were filed in California, Pennsylvania, and Maryland federal courts. Each state is an all-party consent state, meaning that explicit consent is required from both parties prior to recording communications and interactions. Traditionally, this is why consumers are made aware of phone calls being on a recorded line. Other, all-party consent states include Connecticut, Delaware, Florida, Illinois, Massachusetts, Michigan, Montana, Oregon, Nevada, New Hampshire, Pennsylvania, and Washington.

Importantly, to date, federal district court judges in Delaware and Florida have dismissed these lawsuits. Most notably, a Delaware federal court found that there was no injury or invasion of privacy because the sessions were only tracking consumer behavior. In other words, there is no injury in fact if plaintiffs cannot claim that companies are obtaining personal information or attempting to monetize the information collected.

PROFESSIONALS

Molly A. Arranz
Partner

Sofia Valdivia
Associate

RELATED SERVICES

Biometric Privacy

Class Action

Cybersecurity & Data Privacy

Another Data Collection Tool Leads to Privacy Class Actions

However, plaintiffs have also garnered some recent wins. Last year, the Third Circuit found the transfer of consumer data from a business's website to service providers through session replay tools was considered "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.

There's no prevailing view on the issue, and this likely means more class action lawsuits based upon session replay tools. These wire-tapping lawsuits should serve as a reminder, if not a warning, for companies to gain a deeper knowledge about the technology they use. Keep in mind the following:

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 consumer data.** What often makes data privacy tricky to navigate is that there is no one size fits all approach when it comes to compliance efforts. The type of disclosures for your company will depend on a variety of factors such as from where the data is coming, how it is being collected, what is being collected, and more. And as we've seen with these recent class action lawsuits, the laws and legal recommendations are only continuing to evolve. Businesses need to have a comprehensive understanding of what data they are actually collecting and how it is being used to ensure proper consent gathering and privacy disclosures are in place.
3. **Evaluate the data privacy risks you actually *do have.*** These lawsuits are brought against a backdrop of growing concern over whether companies are systematically analyzing, identifying and minimizing the data protection risks of the e-commerce projects they are launching. While you consider the consumer consent gathering on the front-end, take time to assess that each department knows its data protection obligations.