CARLTON FIELDS

Website Data Practices Fueling Privacy Class Actions: Six Tips for Reducing Risk

January 24, 2023

Website tracking technologies have become ubiquitous as a means for companies to monitor traffic to their websites and enhance the user experience. Class actions alleging insufficient notice and consent related to those same technologies, however, have also become ubiquitous. Worse, many of those lawsuits include substantial claims for statutory damages and attorneys' fees. The class actions repurpose old laws, such as those prohibiting wiretapping or eavesdropping, and apply those provisions to argue that companies' websites are violating website visitors' rights. Here, we outline the technologies at play, the emerging risks, and how companies can mitigate those risks. **The Technologies** Website operators use a variety of technologies to gather information regarding consumers' use of their websites. These technologies can serve many purposes, from basic website operation to an important element of targeted advertising campaigns. Two website technologies have recently come under particular fire in litigation: (1) session replay technology, which records an individual's browsing session and interactions with the website; and (2) the disclosure of website video-viewing data for targeted advertising purposes. In these instances, website operators might share information on a particular individual's viewing, or interaction with, a video on a website to identify promising leads for advertisements (e.g., a consumer who has watched a video regarding a particular product may be targeted for further advertising concerning that product). **The Litigation Risk** *Session Replay Technology* Plaintiffs alleging privacy violations based on session replay technology have alleged that website operators are required to provide:

- Pre-recording pop-up messages alerting website visitors that their website browsing session is being recorded; and
- Specific disclosures in the companies' website privacy policies.

Plaintiffs portray failure to provide the above as actionable under various state wiretap laws, invasion of privacy claims (both common law and statutory, such as pursuant to California's Invasion of Privacy Act), and as an unfair trade practice. These claims are repurposing and expanding on the

same theories previously used to allege insufficient notice and consent related to website cookies. Many of these claims provide for statutory penalties and attorneys' fees. *Digital Advertising and Video-Viewing Data* Meanwhile, plaintiffs attacking website video viewing data allege that any disclosure of their viewing of a video on a website, including through use of such tools as Google Analytics and Facebook pixel, requires informed, written consent. Under this theory, failure to secure such consent constitutes a violation of the Video Privacy Protection Act of 1988 (VPPA). These claims gained particular traction in late 2022, after one such claim survived a motion to dismiss. Although the VPPA has several exceptions, these exceptions have not yet been applied to current technologies. Aggressive plaintiffs are sending demand letters to operators of websites that include videos, much like communications sometimes sent alleging violations of the Americans with Disabilities Act. The letters commonly allege that the website has been sharing video viewing data and demand compensation. For health care providers and their business associates, plaintiffs also commonly allege that any failure to provide adequate notice and secure requisite consent for a disclosure also violates the Health Insurance Portability and Accountability Act (HIPAA). Such claims are likely to specifically cite to the Department of Health and Human Service's Office for Civil Rights' recent guidance regarding tracking technologies. Although HIPAA does not provide private plaintiffs with a private cause of action, plaintiffs commonly allege HIPAA violations as part of other claims.
Six Steps to Reduce Risk: We have found that the following steps reduce the risk of litigation stemming from use of these technologies:

1. Take an inventory of the technologies in use on your websites, the data flows involved, and the optional settings available.
2. Educate your team, particularly colleagues in IT and marketing, to the associated requirements and risks involved in different technologies, settings, and data practices.
3. Review your existing privacy notices and processes for documenting consent, and if appropriate:
    - bolster them, even if not legally required; and
    - revise any language that plaintiffs may allege has misrepresented your data collection, use, or disclosure practices, and their options regarding the same.
4. Negotiate vendor contracts to favorably allocate responsibility and risk.
5. Revise website terms of use, and processes for securing acceptance of the same, to maximize the enforceability of arbitration and class action waiver provisions.
6. If you receive a demand letter, carefully review the allegations relative to your website practices and discuss your options with knowledgeable counsel.

Authored By

Patricia M. Carreiro

Related Practices

Cybersecurity and Privacy
Class Actions