Website Tracking and Privacy Policies at Issue in Two New Pennsylvania Court Cases

PUBLISHED ON
December 13, 2022

Two class action lawsuits filed in the last month in Pennsylvania federal court bring to light the perils of using website tracking software. In each of the cases, one against retailer Bloomingdale's and the other against insurer Liberty Mutual, the class action plaintiffs allege that these defendants violated Pennsylvania's Wiretapping and Electronic Surveillance Control Act by using third-party website tracking software on their websites to record and track website visitors' use of the websites without the express knowledge or permission of those visitors.

The website tracking software at issue, Datadog and ClickTale, are widely used by businesses to collect detailed website visitor data, recording each click and keystroke a visitor may make on the website. The software is akin to "spyware" and provides website owners the opportunity to view an entire "session replay" of a visitor's use of the website. The legitimate purpose of the software includes allowing the website owner to discover and fix broken or dysfunctional website features and to enhance visitors' experience using the website. However, the plaintiffs in these cases allege that the breadth of data collected by the websites using the software "far exceeds the stated purpose of the class members' expectation when visiting the websites." The plaintiffs in these cases argue, among other things, that both Bloomingdale's and Liberty Mutual fail to adequately warn its visitors, including the lack of immediate access to the websites terms of use or privacy policy prior to the use of the website and completion by the visitors of the websites' online forms.

Similar cases were brought and are still being litigated in other jurisdictions, including suits brought this week in California (against Ulta and Bass Pro Shop), last month in Florida (against Home Depot) and California (against Papa Johns), and in October in Massachusetts (against Goodyear). Another similar case was recently dismissed in Florida (against Costco). These suits, including those against Bloomingdale's and Liberty Mutual which may also be dismissed, serve as a necessary reminder to businesses regarding the use of website tracking software and the related disclosure to website visitors of a website's collection of visitor information.

Consumer privacy in the United States, including the privacy of information collected on websites, is governed by a patchwork of state and federal laws and regulations. Most notably, the Federal Trade Commission Act, and its state-equivalent consumer protection laws, including the Unfair Trade Practices and Consumer Protection Law in Pennsylvania, regulate unfair and deceptive commercial practices. These laws and regulations have been interpreted to require businesses to accurately warn website visitors of its information collection and sharing practices (typically in the form of privacy policies) and provide adequate protection of personal information. A business's failure to comply with these laws and regulations can result in steep fines and penalties, along with possible liability to website visitors for damages caused by such non-compliance. Now, compounding the risk to businesses seems to be this possible violation of state wiretapping laws when using website tracking software

without full and proper disclosure to website visitors.

To guard against this liability, businesses should ensure that their marketing operations (which often drive the desire to use website tracking software) coordinate an impact assessment with its information technology/security and privacy functions before launching the use of website tracking software. This should include a more than surface-level understanding of how the software will collect and use visitor information, along with the use of a clear, conspicuous, and comprehensive website privacy policy that serves to expressly advise visitors of the type of information it collects, how it collects it, and how it intends to use it. This may include the determination of whether visitors should be required to affirmatively consent to the collection of its information by tracking software, as these cases suggest are necessary. If a business has no terms of use or privacy policy or relies solely on a "canned" privacy policy that does not accurately depict its collection or sharing practices, it could find itself facing a lawsuit of this kind, along with a long, expensive uphill legal battle.

If your business would like to review this issue further, please contact Partner Don Geiter. Don is a Certified Information Privacy Professional (U.S.) (CIPP/US) and leads the firm's Cybersecurity Service Team.

WRITTEN BY:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com