Proskauer

Privacy Class Action Spotlight: Latest Wave of Wiretap Class Actions Continues Despite Dismissals as Plaintiffs Try New Approaches

Proskauer on Privacy on **December 21, 2023**

- Over a hundred cases are pending from the wave of privacy class actions that commenced last year alleging violations of state wiretap statutes based on use of website session replay, chatbot and pixel technologies.
- Plaintiffs' firms are continuing to file new cases based on chatbot and pixel tech despite an increasing number of dismissals while also trying new approaches focused on email marketing tech and identity graphing.

There are now over a hundred cases pending from the wave of privacy class actions that commenced last year alleging violations of state wiretap statutes based on use of website session replay, chatbot and pixel technologies. The plaintiffs' bar was emboldened to take another run at these privacy "gotcha" lawsuits focusing on common website tools after two circuit court decisions from 2022 – *Javier v. Assurance IQ, LLC* from the Ninth Circuit and *Popa v. Harriet Carter Gifts, Inc.* from the Third Circuit – rejected consent and "party to the communication" defenses asserted by defendants respectively under the California Invasion of Privacy Act ("CIPA") and the Pennsylvania Wiretapping and Electronic Surveillance Control Act.

Dismissals of Website Technology CIPA Cases

Although the Ninth Circuit made clear that consent obtained after a user has already begun interacting with a website will not hold water as prior consent under CIPA, California courts are generally citing other grounds for dismissing CIPA cases based on website session replay, chatbot and pixel tech. These include (a) the "party exception" (holding that parties that are the intended recipients of a user's communications are excepted from being considered "eavesdroppers" or "wiretappers" and website tech providers fall within the "party" exception as extensions of the website publisher (with the noted exception being cases where a tech provider uses tracking data for its own purposes)); and (b) a finding that the information shared is not (i) "content" (at least with respect to technical information such as IP address, browser and device type, time and duration of a website visit), (ii) "in transit" or (iii) "intercepted." Some California courts have also concluded that CIPA does not apply to web-based communications at all but rather only to communications occurring over telephones.

Despite the failure of many of these cases on 12(b)(6) motions, we are continuing to see new cases being filed on an almost daily basis under CIPA focused on chatbots and pixel technologies, as several plaintiffs' firms have been taking an assembly-line approach to filing these cases, reducing in some cases their effort in customizing each complaint to no more than changing the name of the defendant and the website URL.

These wiretap cases follow the common playbook of plaintiffs' counsel with privacy class actions – testing to see whether they can dust off pre-digital age laws and persuade courts that these laws should apply to modern technologies never contemplated when the laws were enacted. Fortunately for the companies targeted in these cases, despite the Ninth and Third Circuit decisions, many of the cases that have reached the 12(b)(6) decision stage are failing, and an increasing number of plaintiffs are choosing to abandon cases even after being granted leave to amend. But not to be deterred, plaintiffs' firms are continuing to file new cases almost daily based on chatbots and pixel tracking while also trying out new approaches based on email marketing tech and identity graphing, undoubtedly hoping this shift will better position them to parry the defenses being raised.

Hedging Their Bets: New Theories Emerge

With so many of these website tech wiretap cases dying on the vine, new theories are emerging that could lead to a possibly more troublesome branch of these complaints. In mid-September, a plaintiffs' firm filed a complaint against The Gap, Inc. asserting a CIPA violation based on use of analytics software in Banana Republic email marketing messages. *Ramos v. The Gap, Inc.* The technology at issue in the complaint is analytics software commonly used in the retail sector to track email marketing campaign effectiveness by measuring email opens, conversions, and other standard campaign measurement statistics. The complaint alleges that this email campaign analytics tool violates CIPA by allowing The Gap to "secretly observe and record the interactions of Defendant's customers when they open and/or click on the Content of the Emails and the landing pages of Defendant's Website in real-time." In addition to pleading violations of CIPA, the complaint also asserts causes of action under California's Unfair Competition Law and penal code §§ 484 and 496 (Statutory Larceny).

This focus on email marketing tracking appears to be picking up steam as two new cases, *Mills v. Saks.com LLC* and *McGee v. Nordstrom Inc.*, were recently filed by the same plaintiffs' firm that filed *Ramos v. The Gap*, though rather than asserting wiretap violations, these complaints assert causes of action under Arizona's Telephone, Utility and Communication Service Records Act, a law that "prohibits procuring or attempting to procure the communication service records of email recipients without their authorization." The complaints specifically allege that the defendants "embed trackers within…emails…[that] record whether and when subscribers open and read their messages… [without] receiv[ing] subscribers' consent to collect this information."

In addition to shifting the focus to email marketing tracking, the effort by plaintiff's lawyers to keep the wiretap case train chugging along now also includes another tech angle. In mid-November, a complaint was filed against Cart.com, Inc. based on alleged use of identity graphing technology on the Juicy Couture brand website. *Diaz v. Cart.com, Inc.* In the complaint, the Plaintiff alleges that the Defendant "secretly deployed spyware on its website…in an attempt to de-anonymize every visitor such that each visitor's identity and browsing habits can be monetized and shared with various third parties." The Plaintiff further alleges that use of "'identity resolution' malware tools" are a violation of an internet user's "right to remain anonymous" and asserts both a CIPA wiretap cause of action as well as a cause of action alleging violation of the California Comprehensive Computer Data and Access Fraud Act.

Although the plaintiffs' bar's latest case theories targeting email marketing analytics and identity resolution technologies should be subject to existing defenses, they are nonetheless developments to keep in mind and proactively prepare against. We recommend organizations conduct a review of these technologies used by their teams and the vendor agreements for that tech. In addition to ensuring that vendors are not permitted to use user data for their own purposes, there are a variety of approaches organizations can consider to mitigate the risk of being caught up in what could prove to be a fresh round of wiretap complaints, many of which are dependent upon the types of technologies in play and the compliance tools and processes an organization is currently deploying.

If your organization needs assistance assessing its risk posture with respect to this new case theory and potential mitigation steps, please reach out to our Privacy & Cybersecurity Practice Group co-heads Leslie Shanklin and Ryan Blaney You may also reach out to litigation partners Baldassare Vinti, David Fioccola and Jeff Warshafsky for class action litigation defense strategy.

View Original