Insights, News & Events

GROUNDBREAKING CLASS CERTIFICATION DECISION IN WEBSITE TRACKING CASE SERVES AS WAKE-UP CALL FOR BUSINESSES: PROACTIVE STEPS YOU CAN TAKE

Insights
Dec 18, 2024

In what appears to be a first-of-its-kind decision, a California federal court just granted class certification in a wiretapping claim brought against a website operator that used third-party technology to track users' activity. While wiretapping suits filed against businesses that host third-party cookies, pixels, and other website tracking technology have grown exponentially in recent years, most of these suits typically resolve through settlement or arbitration. However, the groundbreaking November 26 ruling from the Northern District of California that certified a class alleging California Invasion of Privacy Act (CIPA) violations serves as a wake-up call to businesses across the country. What do businesses that utilize third-party technology on their websites need to know about the ruling – and what should they do about it?

What Happened?

In *Torres v. Prudential Financial, Inc.*, the court certified a class of California individuals who visited Prudential.com between November 2021 and December 2022 and provided personal information – and for whom a TrustedForm Certificate URL was generated for that website visit.

The individuals who brought suit allege the website operator (Prudential) and its third-party marketing software platform (ActiveProspect) violated the wiretapping provision of CIPA. This broad statute creates liability for anyone who reads, attempts to read, or otherwise learns the contents of any

Related People

Catherine M. Contino
Associate
610.230.6109

Usama Kahf, CIPP/US
Partner
949.798.2118

communication made over any "wire, line, or cable" without full consent from all parties. A groundbreaking 2022 federal appeals court decision extended the reach of this statute to website usage.

During the class period, Prudential's website enabled users to obtain a quote for life insurance. The company used ActiveProspect's TrustedForm script as part of the website's source code, which Plaintiffs allege enabled ActiveProspect to intercept and record visitors' real-time interaction with the form. ActiveProspect allegedly used the data it collected to create a "session replay," which is a recreated video recording of the user's real-time interaction with the form. Plaintiffs allege that they did not consent to the recording of their interaction with a third party when they completed the form, which required visitors to enter information regarding their demographics, family, situation, and medical history.

What is Class Certification?

Class certification is the way a court determines whether a lawsuit can go forward to trial as a class action. In federal court, the requirements for class certification are set out in Rule of Civil Procedure 23. A plaintiff seeking certification of a class must show:

- the class is so numerous that joinder of all members is impracticable;
- there are questions of law or fact common to the class;
- the claims or defenses of the representative parties are typical of the claims or defenses of the class; and
- the representative parties will fairly and adequately protect the interests of the class.

The Decision

One of the requirements for class certification that Plaintiffs must show is that the factual and legal issues can be determined on a class basis and don't require individualized inquiry. Defendants argued that the issues of implied consent, class member eligibility, and location of the alleged interception in California require individualized inquiry into each class member's circumstances.

The court rejected this argument.

Service Focus

Consumer Privacy Team

Digital Wiretapping Litigation

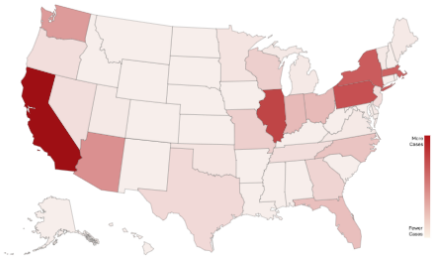
Litigation and Trials

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Wiretapping Litigation Map



- It found that each of these potential issues could be resolved through common proof or manageable methods, like affidavits or cross-referencing data.
- It found that the question of whether a reasonable user would understand Prudential's privacy policies is a common one that could be resolve with class-wide proof rather than through individualized inquiry.
- The court also found that the method for identifying class members can be achieved through cross-referencing data and that identifying class members is not grounds for denying class certification.
- Finally, the court noted that identifying class members' location would be possible through affidavits and necessary cross-reference if there was a dispute as to where a class member resides.

Impact of Decision

The court's certification of the class is significant, as it signals a willingness of judges to accept an expansion of the scope of CIPA to apply to a user's interactions with a website. As noted above, the federal appeals court covering California has extended the state's wiretapping statute to include website activity. There is a split in authority across the country, however, as Massachusetts' Supreme Court recently refused to extend its state wiretapping law to websites.

However, just because a class is certified does not mean that plaintiffs will be successful in garnering the common proof necessary to win at trial. Rather, it gives them the opportunity to collect evidence in support of their claims on a class wide basis. Defendants could request that the court decertify the class, which means withdrawing or revoking the certification of the order that granted certification of the class. Motions seeking to deny certification most often occur after class discovery is completed. The most common grounds for a motion denying class certification are that plaintiffs have sought to build an overly broad class or asserted class allegations with insufficient specificity or factual support.

Businesses everywhere should be following this case and whether it proceeds to trial, as CIPA provides statutory damages from $5,000 per violation to three times actual

damages. Potential damages can skyrocket even with a relatively small class.

5 Data Privacy Compliance Steps to Consider Taking Now

As wiretapping claims (and tracking technology) are quickly becoming commonplace for businesses across the country, businesses should closely review their websites to ensure what kind of tracking technology they employ and whether appropriate disclosures are displayed. Here are some steps you can consider:

1. **Review Your Website**: Closely review your website to evaluate the pixels, web beacons, cookies, and other tracking tools being used. Identify the data each tracking tool discloses and any third parties receiving it. Ascertain what third parties are doing with the data once they receive it.

2. **Display Appropriate Disclosures**: *Before* the consumer provides any information on your website — for example, through a search bar, a contact form, or chat feature — review your website disclosures to ensure they adequately describe the parties to the communication, who will receive the data, the further use (if any) of the data, and where consumers can access information about your privacy and data use practices.

3. **Ensure Third-Party Compliance**: Be proactive by periodically reviewing your third-party providers' data privacy practices to ensure they comply with legal obligations as well as your company's policies.

4. **Consider Privacy Preserving Technologies**. Many of the state comprehensive consumer privacy laws either recommend or require (in certain circumstances) the adoption of privacy preserving technologies on websites, like Global Privacy Controls (GPCs) or HTTP header field or JavaScript objects. Such technology could allow a user to set their browser to send an automatic signal to each website they visit telling the website that this user does not wish to have any data that can identify them collected or disclosed through cookies. If your website enables or accepts GPCs, the website would automatically accept the user's preset signal and comply with the user's choice without requiring the user to further select cookie choices upon navigating to the website. Depending on your organization's data practices, you may be required, or

may consider, implementing automated ways to acknowledge consumer opt-out preference signals.

5. **Seek Legal Counsel**. Your Fisher Phillips attorney or one of our privacy counsel can help you effectively and comprehensively develop a compliance plan.

Conclusion

Fisher Phillips will continue to monitor developments in this area. We will provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You should also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate these developments. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Consumer Privacy Team.