Big Wiretapping Win for Businesses in Massachusetts Data Privacy Case: 5 Compliance Reminders for Website Tracking Software

Insights
10.24.24

Businesses that use website tracking software to monitor activity for marketing purposes must comply with a growing list of state laws – but does that include a nearly 60-year-old Massachusetts law requiring consent to record or listen to phone calls? The Massachusetts Supreme Judicial Court just delivered good news today to businesses that use such technology (like Google Analytics or social media pixels) and the firms that create it. The court held a hospital's use of third-party website tracking software does not violate the state's Wiretap Act, which imposes criminal and civil penalties for intercepting certain communications. Web browsing, or a user's interaction with a website, is not a covered communication under the act, as it is not a person-to-person communication. Will this decision impact claims based on use of website cookies under wiretapping laws in other states? Here's what businesses across the country need to know about the ruling and five steps you can take to comply with evolving data privacy rules.

What Happened?

- **Patient Sued Hospitals:** In *Vita v. New England Baptist Hospital*, a patient brought a proposed class action under the Massachusetts Wiretap Act, claiming that two hospitals collected and shared her information with third parties for marketing purposes without her consent.
- **Web Browsing Activities:** The patient alleged that she accessed and reviewed public information on the hospitals' websites, such as doctors' profiles, medical symptoms and conditions, and procedures. She claimed these interactions with the websites were "wire communications" protected by the act.
- **Ambiguous Language:** The Massachusetts Supreme Judicial Court noted that the term "communication" in the statute is ambiguous, so the hospitals were entitled to "the benefit of any rational doubt."
- **The Meaning of "Communication":** According to the court, "communication" includes messages and conversations between people in person, on the phone, and through e-mail, text message, chat, instant message, or the equivalent.
- **Web Browsing is Different:** In this case, the patient's complaint involved interactions with the hospitals' website, not their staff. "When a user browses a public website, and accesses databases and other information readily available to anyone on the Internet, the user is not

databases and other information readily available to anyone on the internet, the user is not speaking or messaging with another person but rather interacting with the website; the user is also not engaged in personal conversation or messaging but rather browsing and interacting with the published information on the website," the court noted.

- **Court Sides with Hospitals:** "Ultimately, we cannot conclude that the wiretap act unambiguously prohibits and, indeed, criminalizes the interception of web browsing activity," the court found. Critically, it found a big difference between interactions on a public website and private conversations in a house or on the telephone, the latter being the intention of the act.
- **But Watch for More Developments:** Although the Massachusetts Supreme Judicial Court held tracking software use does not violate the state's Wiretap Act, the court acknowledged that there may be other claims outside of the Wiretap Act, and businesses still should consider the host of privacy laws regarding tracking website user interactions. Moreover, whether the Massachusetts Legislature will respond and broaden the wiretap law in the future is not yet known. Additionally, while this case resulted in a positive outcome for businesses that develop and use online tracking software, courts in other states have reached different conclusions under various state privacy and wiretap laws. So, you should closely track developments in this area as rules evolve.

What Specific Developments Should Healthcare Businesses Track?

- **Claims Involving Medical Information:** You should note that this case did not address other legal theories being asserted against healthcare businesses for use of this technology on their websites, including novel theories that data disclosure about a user's interaction with a healthcare website may be a data breach of "medical information." We're even seeing data breach claims just based on the fact that the user visited the site (coupled with device or browser specific data that third parties, such as data brokers, can use to identify the person and track them across the internet). You can read more about that issue here.
- **Key Takeaway:** You should recognize — especially when users go to your website to find providers, get info on healthcare services, or log into a patient portal — you may see more claims that third-party cookies that disclose browsing activity can result in a data breach of medical information. Follow our steps below to help ensure compliance.

5 Data Privacy Compliance Steps to Consider Taking Now

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 parties receiving it. Ascertain what third parties are doing with your 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. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Consumer Privacy Team.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Usama Kahf, CIPP/US
Partner
949.798.2118

Email

Danielle Kays
Partner
312.260.4751
Email

Joshua D. Nadreau
Regional Managing Partner and Vice Chair, Labor Relations Group
617.722.0044
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Industry Focus

Healthcare

Related Offices

Boston