GUNDERSON DETTMER

Data Privacy Insight: Notice of Substantial Increase in Legal Demands Regarding Website Technologies: How to Immediately Reduce Your Risk of Receiving a Claim

Insights
March 27, 2024

Over the past year, hundreds of companies have become targets of legal claims regarding their use of certain website technologies – specifically advertising pixels (such as the popular Meta Pixel), session replay technology, SDKs, chatbots, and other tracking technologies. Creative plaintiffs' lawyers representing website and mobile app users have leveraged older wiretapping and privacy laws, such as the California Invasion of Privacy Act and the Video Privacy Protection Act, that provide broad private rights of action and statutory damages in order to extract settlements from companies which are generally not available under more recent U.S. state privacy laws.[1]

While most of the lawsuits are still pending trial or being quickly settled, we expect that many of our clients may be at risk of being targeted with such a claim or a demand letter from a plaintiffs' law firm. We strongly advise that you promptly assess your use of pixels and other tracking technologies, and implement appropriate risk mitigation strategies, as further described below. Please also reach out to your Gunderson attorney for immediately actionable steps to mitigate your risk.

What Technologies Have Been Targeted?

- **Meta Pixel:** The Meta Pixel is a commonly used piece of code deployed on a website to measure the effectiveness of an advertisement by understanding the

actions website visitors take on that website. The code can send information about how users interact with the website back to Meta, which allows not only the website owner, but also Meta, to use and analyze this data to better target ads.

- **Chatbots:** Chatbots are programs or software that automatically respond to messages sent via a website's chatbox, emails, social media messages, or text messages. Typically, websites use chatbots to respond to routine website visitor questions and inquiries.

- **Session Replay:** Session replay technology reproduces a visitor's website or app interaction exactly how the visitor experienced it. This may include the visitor's view (e.g., what's on the browser screen), visitor input (e.g., keyboard and mouse strokes), and logs of network events. Session replay technology can help improve customer experience on a website or app, and can also be used to study customer behavior and preferences.

- **Software Development Kits (SDKs):** SDKs are a set of tools, libraries, documentation, and sample code provided by a software company or platform to assist developers in building applications for a specific software framework, platform, operating system, or hardware device. For example, the Facebook SDK is provided by Meta to help developers integrate their applications with the Facebook platform. The Facebook SDK includes libraries, APIs, development tools, documentation, and sample code that enable developers to incorporate features such as social sharing, authentication, user profile information, and analytics into their applications.

What are the Legal Theories behind these Demands?

- **California Invasion of Privacy Act ("CIPA") and other state privacy and consumer protection statutes:** Plaintiffs' lawyers have alleged that sending information about the website visitor to Meta, and other third party recipients, without the visitor's knowledge or consent constitutes wiretapping under CIPA. Recently, California plaintiffs' firms have introduced a new theory, alleging that companies violated CIPA by installing tracking technologies that act as an illegal "pen register" (a device that records the dialing/routing information of communications but not the content), thereby monitoring and tracking the website visitor's activity without consent or a court order. For example, in *Greenley v. Kochava, Inc.****[2]***, the plaintiff alleged that defendant's SDKs secretly collected data from app users and that the installation of the SDKs is an illegal "pen register." Some attorneys view this as potentially a stronger legal theory than wiretap claims under CIPA. The main reason that CIPA class actions have gained traction is the statutory damages of $5,000 "per violation," which can mean hundreds of millions

of dollars for a single class action case. There are also similar statutes in Pennsylvania, Florida, Illinois and Wisconsin.

- **The Video Privacy Protection Act ("VPPA"):** Recent lawsuits apply the VPPA, a 1988 statute intended to protect an individual's video rental history, to website operators who offer video content (whether first party or third party videos) in connection with tracking tools such as the Meta Pixel. Plaintiffs' firms have argued that by using the Meta Pixel or other tracking technologies, a website operator reveals to Meta and other recipients a website visitor's activities, including information about viewed video content. Like CIPA, VPPA litigation is attractive because it includes statutory damages of $2,500 "per violation," which opens the possibility of large class action settlements.
- **Other Creative Legal Theories:** Plaintiffs' firms have also brought actions under other federal privacy and wiretap laws, such as the Federal Wiretap Act and the Electronic Communications Privacy Act, as well as claims under the constitutional right to privacy, right of publicity statutes, and invasion of privacy torts.

What are Some Mitigation Tactics?

1. **Assess Your Website Regularly**

Regularly assess which tools you are using on your websites. Are you using Meta pixels, chat bots, and/or session replay technology? Do you have video content on your website in connection with Meta pixels or other third-party marketing/analytics tools? What other tracking technologies fire on your websites? These regular assessments are crucial in identifying any potential privacy risks and taking proactive measures to address them. Also consider implementing a review process before new tracking tools are added on your website, and removing any riskier trackers that do not provide enough of a benefit to your organization to justify the risk.

1. **Update Website Terms of Use and Privacy Policies**

Transparency is key, not only in building trust with users, but also in complying with various consumer and privacy laws. Your website terms of use and privacy policies need to include disclosures about the types of tracking technologies used, the data collected, and how such data is used. These policies need to be easily accessible to users, prominently displayed on your website, and written in clear, understandable language.

1. **Obtain Informed Consent**

Consider implementing mechanisms to obtain explicit consent from users before collecting any personal data through pixels or tracking technologies. This may be achieved through a properly executed and user-friendly banner that clearly discloses the presence of pixels and tracking technologies, obtaining user consent before any riskier trackers are deployed, and providing a link to your privacy policy on the homepage. Make sure that your banner is tailored to minimize the risk of the particular tracking technologies used on your website.

1. **Provide User-Friendly Opt-Out Mechanism(s)**

Provide users with options to control their privacy settings, such as opting out of certain types of tracking, adjusting cookie preferences, and honoring preference signals such as Global Privacy Control signals ("GPC"). Specifically, if you are deploying tracking technologies in a way that constitutes a "sale" under the California Consumer Privacy Act ("CCPA"), then you need to provide a compliant way for visitors to opt out of such sale. Respect user preferences regarding privacy and honor their choices promptly and transparently.

1. **Chatbot Disclosures**

If you use chatbots on your website, include a disclosure to that effect at the first prompt of the chat feature. Additionally, from a user-interface perspective when designing your chat feature, consider including clear visual signs that the user is interacting with a bot, such as a robot icon in the chat box and/or giving the bot a name such as "virtual bot assistant." Note that California's **"Bot Law"** prohibits communicating with a California resident via a bot with the intent to conceal the artificial identity of the bot in order to influence a commercial transaction.

1. **Review Third Party Agreements**

Review your agreements with third party technology providers to ensure appropriate limitations on their access to, and use of, any personal information collected on your website are in place. This is also an important step in assessing whether any of your data sharing constitutes a "sale" under U.S. state privacy laws.

1. **Consider Data Minimization Strategies**

Consider adopting a data minimization approach, collecting only the data necessary for your website's functionality or specific business purposes. Avoid collecting sensitive personal information unless absolutely necessary, and securely dispose of any unnecessary data.

1. **Train Employees on Tracking Technologies and Data Privacy**

Educate your team on the importance of data privacy and their role in safeguarding user information. Provide training on best practices for handling data, responding to user inquiries, and complying with privacy regulations.

How can GD help?

If you have any questions regarding this client alert, or your company needs assistance with this topic, please reach out to your Gunderson Dettmer attorney or contact any of the following members of our data privacy group:

Anna Westfelt	(650) 463-5367	awestfelt@gunder.com
Cecilia Jeong	(646) 490-9094	cjeong@gunder.com
Frida Alim	(415) 801-4921	falim@gunder.com
James Gately	(617) 648-9313	jgately@gunder.com
Jerel Pacis Agatep	(424) 214 1747	jagatep@gunder.com

---

[1] As of March 2024, there are 13 comprehensive state privacy laws either already in effect or signed to law, including CA, CO, CT, DE, IN, IA, MN, NJ, OR, TN, TX, UT, and VA, with numerous other states having active privacy bills going through the legislative process. The California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, provides a limited private right of action for data breaches involving certain types of more sensitive personal information. Other states have also enacted data specific privacy laws, such as the My Health My Data Act in WA, which does have a private right of action.

[2] Greenley v. Kochava Inc., No. 22-CV-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

Related People

Anna C. Westfelt
PARTNER
P +1 650 463 5367

Cecilia Jeong
ASSOCIATE
P +1 646 490 9094

Frida Alim
ASSOCIATE
P +1 415 801 4921

James W. Gately
ASSOCIATE
P +1 617 648 9313

Jerel Pacis Agatep
PRACTICE INNOVATION ATTORNEY
P +1 424 214 1747

Related Services

Data Privacy

Featured Insights

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding

INSIGHTS

Legal 500 Country Comparative Guides 2025: Venture Capital (Singapore)