iab.

Wiretapping Claims

Litigation Preparation & Defense Toolkit

APRIL 2024

Sponsored by

PERKINSCOIE

Table of Contents

Disclaimer: The information provided in this white paper is for educational purposes only. It is not intended to serve as and should not be relied upon as legal advice. Companies considering their own specific compliance obligations should consult with qualified legal counsel.

The last several years have brought in a wave of lawsuits alleging that the use of session cookies, certain tracking pixels, AI assisted call centers, and chatbots result in the interception of communications in violation of federal and state wiretapping laws.

Session replay cookies record and replay user interactions with a website. The cookie (a small piece of code) collects data about user interactions with a website, such as mouse movements, clicks, form submissions, and keyboard strokes, as well as pages visited, and time spent on the page. The actions are often recorded in a log, heat map, or other video-like recording. Session replay cookies are used to help website operators evaluate the user experience and identify usability issues, such as confusing navigation, broken links, or form submission errors. Session replay cookies can also be used to document compliance (e.g., tracking whether someone accepted cookies or opted-in to data use) and identify potential security issues or fraud.

Chatbots enable website and other platform operators to engage with users to answer questions and provide information and technical support. Companies may retain records of the communications between consumers and chatbots. Like recording customer service calls, these records are typically used to analyze and improve the chatbot functionality.

Pixels generally collect information about users' website interactions (page views, clicks, purchases, etc.). Social media pixels, which have been the subject of several recent actions,[1] facilitate the disclosure of a website users activity and links that activity with the user's proprietary social media ID – and thereby provide the social media company with information about the user's website activities.

Violations of the Federal Wiretap Act of 1968 (FWA) can incur damages of up to $10,000 per violation.[2] Fines under similar state laws range from $1,000 to $50,000 per violation, depending on the state.

This Toolkit provides an overview of these wiretapping claims, an outline of the key elements of each claim, a description of the successful and unsuccessful defenses, and proactive next steps to take to avoid a complaint.

[1] *See, e.g., Louth v. NFL Enterprises LLC,* 1:21-cv-00405-MSM-PAS, 2022 WL 4130866 (D.R.I. Sept. 12, 2022); *Carroll v. General Mills, Inc.*, 2:23-cv-01746, 2023 WL 4361093 (C.D. Cal. June 26, 2023); *Feldman v. Star Tribute Media Co LLC*, 22-cv-1731 (ECT/TNL), 2023 BL 73142 (D. Minn. 2023).; In *re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218 (N.D. Cal. Dec. 22, 2022); *Kurowski, et al., v. Rush System for Health d/b/a Rush University System for Health*, No. 22 C 5380, 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023)

[2] 18 U.S.C. § 2520(c)(2) (2022)

I. Overview: What Is "Wiretapping"

a. Federal Wiretapping Act: Electronic Communications Privacy Act of 1986

The Federal Wiretap Act of 1968 ("**FWA**") was initially focused on regulating law enforcement's use of wiretaps, which intercept wire communications. The Electronic Communications Privacy Act of 1986 ("**ECPA**") amended the FWA to include electronic communications, which are all non-wire and non-oral communications (i.e., signals, images, data) that can be transmitted through a wide range of transmission mediums (e-mail is an example of electronic communication).[3] ECPA applies to all persons (not just law enforcement) and prohibits intercepting and disclosing the contents of wire, oral, and electronic communications.[4]

What activities are regulated by ECPA?

□ Interception (including attempted interception) of wire, oral, or electronic communications.

□ Using (including through another party) an electronic, mechanical, or other device to intercept any oral communication.

□ Using or disclosing the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained in violation of the FWA.

*Notably **ECPA and FWA requires only one-party consent**. An individual can record her conversation without violating federal law. In contrast, analogous state statutes in California, Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Oregon, Nevada, New Hampshire, Pennsylvania, and Washington require ALL parties to the communication to give prior consent to an interception. Recent class actions have focused on states, such as California and Pennsylvania, which require two-party consent.

b. California Invasion of Privacy Act ("CIPA")

CIPA, which went into effect in 1967, was enacted to address illegal eavesdropping and wiretapping of private confidential conversations. The law was largely drafted to address communications via telephone, rather than Internet communications, which didn't exist in in 1967. While CIPA is a criminal statute under the California Penal Code, it also creates a civil private right of action for violations of the statute.[5]

What activities are regulated by CIPA?[6]

□ Making an **unauthorized connection** (including electronically) with a telegraph or telephone wire (wiretapping); OR

□ Reading or attempting to **read or learn the contents of a message or communication** while that message is "in transit" or simultaneously without the consent of all parties; OR

[3] 18. U.S. C. 2510(12).

[4] 18 U.S.C. § 2511

[5] Cal. Pen. Code §637.2.

[6] Cal. Pen. Code §631.

- □ Using **any information obtained through eavesdropping/wiretapping**.
- □ Using a pen register or trap and trace device without consent.
- □ **Aiding and abetting** any of the above.

While the text of CIPA focuses on telephone communications, courts have determined that § 631(a) applies to internet communications.[7] Fines for violating CIPA are $2,500 per violation.[8]

In addition to providing for civil penalties, the statute includes a private right of action allowing for $5,000 in statutory damages. An amendment effective January 1, 2017 specified that the statutory damages are "per violation." See Cal. Penal Code § 637.2(a)(1).

c. Pen Register Claims: A New Iteration of Wiretapping Allegations

In 2023, the plaintiffs' bar began experimenting with a new CIPA claim that website operators are using a pen register or a trap and trace device. CIPA Section 638.51 prohibits the installation or use of a pen register or a trap and trace device **without first obtaining consent**. CIPA Section 638.50(b) defines a "pen register" as a device or process that records or decodes outgoing dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted. Similarly, Section 638.50(c) defines a "trap and trace" device as a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication. To put these definitions more simply: a "pen register" records all phone numbers called out from a specific phone and "trap and trace" records all phone numbers coming into a specific phone. Neither a "pen register" or a "trap and trace" records the content of the communications, only to whom they were directed. Thus, with a properly obtained "pen register or a trap and trace device," law enforcement would have a written log of the devices contacted by or to a specific phone or device. Unlike a wiretap, which allows real-time interception of the content of the communications, pen registers and trap and trace devices are limited to the collection of these logs of dialing, routing, addressing, or signaling information.

To date, only one case has formally outlined the elements necessary to establish a claim under Cal. Penal Code Section 638.51: Greenley v. Kochava, Inc., No. 22-cv-01327, 2023 WL 4833466 (S.D. Cal. July 27, 2023). In *Greenley v. Kochava*, the plaintiff claimed that session replay software installed in third-party mobile applications constituted an illegally installed pen register. The defendant moved to dismiss, arguing that its software was not a pen register. After noting that no other court had interpreted CIPA's pen register provision, the court concluded that "software that identifies consumers, gathers data, and correlates that data through unique 'fingerprinting' is a process that falls within CIPA's pen register definition." Greenley, Case No. 22-cv-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023). Accordingly, the court denied Kochava's motion to dismiss.

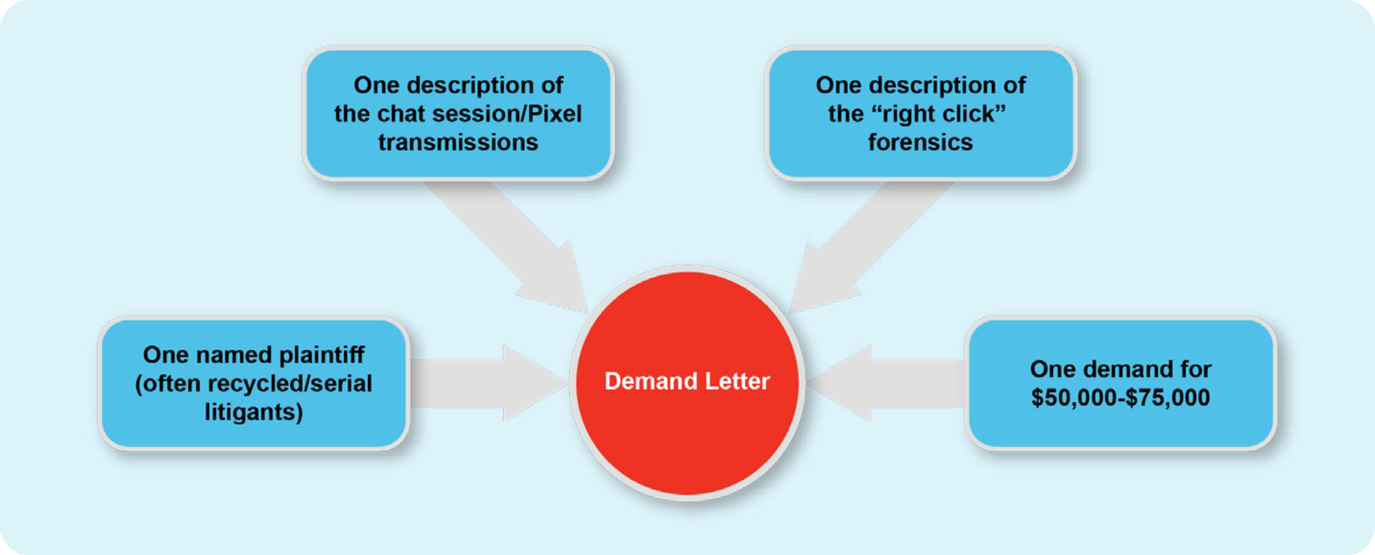
[7] *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 U.S. App. LEXIS 14951 (9th Cir. May 11, 2022) ("Though written in terms of wiretapping, § 631(a) applies to internet communications.")

[8] Cal. Pen. Code §631(a)

The *Greenley* court's interpretation causes significant challenges. All phones and internet-linked devices compile lists of the other devices contacted and contacting them. Such lists are the backbone of "caller ID" and the "back button" in a web browser. Under Greenley, these ubiquitous functions fall within CIPA's definition of a pen register or a trap and trace. Such an expansive interpretation may ultimately be adjudicated on appeal.

***Note: There is an open question as to whether consent is a defense to these claims.**

II. Anatomy of a Claim


One description of the chat session/Pixel transmissions
One description of the "right click" forensics
One named plaintiff (often recycled/serial litigants)
Demand Letter
One demand for $50,000-$75,000

Courts generally apply the same analysis used to evaluate violations of the FWA to determine whether CIPA has been violated.[9]

a. Who Can be Held Liable Under CIPA? Consider Primary Party Exception

To state a claim under the first two clauses of Section 631, a plaintiff must establish that the defendant is a third party. CIPA liability has been held to attach only to eavesdropping by a third party and not to recording by a participant (i.e., the primary party) to a conversation.[10] This is because a party to a conversation cannot eavesdrop on its own conversation. To establish a CIPA violation, there must therefore be a third-party eavesdropper—i.e., a third-party provider of the pixel, cookie, etc.[11] Accordingly, a party cannot be liable for intercepting or eavesdropping on a

[9] *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 517 (C.D. Cal. 2021).

[10] *Warden v. Kahn*, 99 Cal. App. 3d 805, 811, 160 Cal. Rptr. 471 (1979) (finding that Section 631 "has been held to apply only to eavesdropping by a third party and not to recording by a participant to a conversation")

[11] *In re Google Cookie*, 806 F.3d 125, 152 (3d Cir. 2015)] (holding that CIPA claims could be dismissed because the parties were exempted from liability under the Wiretap Act's primary party exception) ("The pleadings demonstrate that Google was itself a party to all the electronic transmissions that are the bases of the plaintiffs' wiretapping claims. Because § 631 is aimed only at 'eavesdropping, or the secret monitoring of conversations by third parties,' we will affirm the dismissal of the California Invasion of Privacy Act [*26] claim[.]")

communication to which it is a party.[12] But because CIPA provides for aiding and abetting liability, a website owner (although a party to a communication) can nonetheless potentially be held liable for allowing a software provider to place a tracking cookie/pixel on its website (subject to certain defenses discussed below).[13]

So, when might a third-party provider of tracking software qualify as a third-party eavesdropper such that the website owner could be subject to aiding and abetting liability? If a vendor is hired to work on behalf of a website owner/operator to help that owner/operator record its conversations, that vendor should be treated as an extension of the website owner/operator, not a third party.[14] However, the analysis is not always straightforward.

The Court will look at several factors to determine whether a vendor is a third party, including the vendor's ability to use the contents of the communication for its own financial gain and whether the recording is simultaneous or second-hand.[15] For example, where Meta was alleged to use GET requests in connection with its Facebook plug-ins to duplicate the contents of a communication and relay it back to a party, the court found that Meta acted as a third party.[16] Where session replay technologies recorded conversations in real time, some courts have been more willing to find that the vendor was acting on behalf of the website and not in violation of CIPA (provided that there was no other indication that the data was being collected and use for independent financial gain). Other courts have found that session replay software providers may constitute a third-party eavesdropper.[17] Ultimately, the court will consider whether the software provider merely records and stores the information for the website operator's use, or if it is able to independently use the data for its own financial gain.[18]

[12] *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 142-43 (3d Cir. 2015)

[13] Cal. Penal Code § 631; *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192, 148 Cal. Rptr. 883, 192 (1978).

[14] *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 606-07 (9th Cir. 2020), cert. denied sub nom. *Facebook, Inc. v. Davis*, 141 S. Ct. 1684, 209 L. Ed. 2d 464 (2021); *Williams v. What If Holdings, LLC*, No. 22-cv-3780, 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022) (Alsup, J.); *Byars v. Hot Topic, Inc.*, No. EDCV 22-1652 JGB (KKx), 2023 WL 2026994 (C.D. Cal. Feb. 14, 2023).

[15] *Yockey v. Salesforce, Inc.*, No. 22-cv-09067-JST, 2023 U.S. Dist. LEXIS 150262, at *8-9 (N.D. Cal. Aug. 25, 2023).

[16] *Davis v. Facebook, Inc.* (*In re Facebook Inc. Internet Tracking Litig.*), 956 F.3d 589, 595 (9th Cir. 2020)

[17] *See, e.g., Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503 (C.D. Cal. 2021)

[18] Williams, 2022 WL 17869275, at *3 ("[A] key distinction is whether or not the alleged third-party software provider aggregates or otherwise processes the recorded information, which might suggest that the software vendor independently 'users' the gathered data in some way."); Byars, 2023 WL 2026994, at *9 (dismissing CIPA claim where the allegations permitted an inference that "Defendant uses a third-party vendor to 'record and analyze its own data in aid of [Defendant's] business,' not the 'aggregation of data for resale,'" which makes the third-party an 'extension' of Defendant's website, not a 'third-party eavesdropper.'"

Practice Pointer:

Graham v. Noom, Inc., 533 F. Supp. 3d 823, 828 – Noom, a website that helps users lose weight, used FullStory's session replay software. Fullstory collects data on website interactions, hosts that data on its servers and allows clients to analyze it. The court noted that there were no allegations that FullStory intercepted and used the data itself or for its own purposes. The court found that FullStory is a service provider, and therefore an extention of Noom and protected by the primary party exception.

Vs.

Davis v. Facebook, Inc. **(*In re Facebook Inc. Internet Tracking Litig.*)**, 956 F.3d 589, 595 (9th Cir. 2020) - The court found that when Facebook embeds its plug-in on third party sites, it creates a duplicate of the conversation (rather than recording the original). The court noted that "simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception." This duplication, in addition to its use of the data to enhance its own user profiles, was sufficient to establish, on a motion to dismiss, that Facebook could be a third party under CIPA.

Key Takeaway: Whether a vendor is a third party will turn on how the data is collected, as well as how it is used by the vendor. The closer the software is to a "tape recorder" that makes simultaneous recordings used solely for the website owner, the stronger the argument that it is not a third party.

What factors determine whether a company is a third party eavesdropper?

□ Does the third party aggregate or use the information independently from the service is providing?

□ Does the third party have any financial gain from use of the data outside of the charge for providing it services?

□ Is the software on one page or the entire website (i.e. is the vendor engaging in "data mining")?

□ Is there an agreement restricting or limiting the use of the data?

□ Is the vendor duplicating the conversation or just recording and transmitting the recording?

□ Is use of the third-party vendor's technology ubiquitous on the internet?

□ Does the third-party vendor "intercept" communications in transit (not just through accessing stored files after a communication has concluded).

b. Do the "intercepted communications" qualify as protected content under CIPA?

As set forth above, Section 631(a)[ii] penalizes a person who "reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication[.]" The Ninth Circuit has held that the "contents" of an online communication under federal wiretap law "refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication."[19]

Thus, CIPA § 631(a)[ii] should only protect the substance of a message, not identifiers and other details. However, the caselaw is mixed on this point. Several judges have dismissed cases involving the collection of keystrokes, mouse click and page views because these pieces of data are not message content that are analogous to the text of an email.[20] Other judges, however, have held that capturing "mouse movements, clicks, typing, scrolling, swiping, tapping, keystrokes, geographic location, IP addresses, and data entry… alongside a video capturing each of Plaintiff's keystrokes and mouse clicks on the website was sufficient to show content at the pleading stage."[21] Arguments that the contents of chatbot communications are protected content under CIPA have been more universally successful.

c. Consent

Section 632 provides that '(a) every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records such confidential communication… shall be punished by fine… or by imprisonment.'"[22] A company will either need to demonstrate consent or that there is no reasonable expectation of privacy in the conversation. Consent should be affirmative and specific to the tracking at issue. Disclosures in privacy policies that are hyperlinked on a website, but do not require a separate opt-in consent are riskier and may be insufficient.[23] However, it is worth noting that in the pixel cases, there is a potential defense under an unpublished Ninth Circuit decision that consent to Meta's policies constitutes sufficient consent.[24]

[19] *In re Zynga Priv. Litig*., 750 F.3d 1098, 1106 (9th Cir. 2014) (contents transmitted by Facebook.com did not include a user's Facebook ID and browsing history when automatically gathered, but it could include messages that stated that information).

[20] *See, e.g., Yoon v. Lululemon USA, Inc*., 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021) ("Yoon alleges that Quantum Metric recorded her keystrokes, mouse clicks, pages viewed, and shipping and billing information and the date and time of the visit, the duration of the visit, Plaintiff's IP address, her location at the time of the visit, her browser type, and the operating system on her device. None of these pieces of data constitutes message content in the same way that the words of a text message or an email do.") (cleaned up).

[21] *Saleh v. Nike, Inc*., 562 F. Supp. 3d 503, 517–18 (C.D. Cal. 2021); see also *Tanner v. Acushnet Co.*, No. 823CV00346HDVADSX, 2023 WL 8152104, at *3 (C.D. Cal. Nov. 20, 2023).

[22] *Rattray v. City of National City*, 51 F.3d 793, 797 (9th Cir. 1994) (quoting Cal. Penal Code § 632).

[23] *Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171, 1178-79 (9th Cir. 2014).

[24] *Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018) (unpublished) ("A reasonable person viewing those disclosures would understand that Facebook maintains the practices of (a) collecting its users' data from third-party sites and (b) later using the data for advertising purposes. Knowing authorization of the practice constitutes Plaintiffs' consent.").

Practice Point:

Yockey v. Salesforce, Inc., No. 22-cv-09067-JST, 2023 U.S. Dist. LEXIS 150262, at *19-20 (N.D. Cal. Aug. 25, 2023) –In a case involving chatbots, the court found that because there was at least one chat portal that did not require consent before use, and it is possible that the plaintiff used that portal, Salesforce was unable to establish consent and the claims survived a motion to dismiss.

Key Takeaway: For chatbots, insert consent to recording language at the top of each chat to established consent.

d. Were the communications intercepted in "transit"?

Under FWA and CIPA, an interception is the acquisition of the contents of any wire, electronic, or oral communication through the use of any electric, mechanical, or other device that occurs during the transmission, not when the communication is in electric storage.[25] Notably, plaintiffs generally have a harder time establishing the interception of communications in transit in the context of chatbots. Bare allegations of recording and creating transcripts have not been sufficient to allege that Plaintiffs' messages were intercepted while in transit.[26] In contrast, the session replay technologies, which record actions in real-time, may satisfy the "in transit" requirements.[27]

That said, some courts have held that, at the motion to dismiss stage, a plaintiff is not expected to prove or even know how and when its communications were captured.[28]

III. Overview of Recent Wiretapping Defenses

Recent Successful Defenses:

□ Participant/Primary party exception. To establish a primary CIPA violation, there must be a third-party eavesdropper—a party to a conversation cannot eavesdrop on its own conversation. Recent successful defenses have established that the third party was an extension of the primary party, because: 1) they were restricted in how their data was used; 2) they were unable to and did not use the communication for their own financial gain; or 3) the recording was simultaneous.

□ Vendor is an extension of the defendant (akin to a tape recorder), not a third-party eavesdropper.

[25] *Gonzalez v. Uber Technologies, Inc.*, 305 F. Supp. 3d 1078, 1086 (N.D. Cal. 2018); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (holding the acquisition of email messages stored on an electronic system, but not yet retrieved by the intended recipients, is not an "interception" under the Wiretap Act).

[26] *Martin v. Sephora USA, Inc.*, No. 1:22-cv-01355-JLT-SAB, 2023 U.S. Dist. LEXIS 55930, at *28 (E.D. Cal. Mar. 30, 2023).

[27] *Saleh v. Nike*, 562 F. Supp. 3d 503, 509 (C.D. Cal. 2021).

[28] *In re Vizio, Inc. Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017).

□ The defendant obtained consent in advance of the recording (ideally via an affirmative consent to a website privacy policy or pop-up/consent banner).

□ With respect to chatbots, they do not intercept communications in-transit.

Recent Unsuccessful Defenses:

□ Passive consent was obtained (where the recording was not disclosed within a chat or was only disclosed in website disclosures without requiring any affirmative consent/action).

□ A vendor that duplicates, rather than simultaneously records communications, is not a third party.

□ The communication was not confidential, when sensitive information (e.g. health data) was recorded.

□ Consent was obtained after recording or interception started.[29]

IV. Proactive Steps to Reduce the Risks from Litigation

Despite the proliferation of class action litigation, there are numerous proactive measures that organizations can take to mitigate the risks associated with cookies, pixels, chatbots, and the like. The commonality across these risk mitigation steps is adherence to good "privacy hygiene" based upon well-established principles like transparency, choice, use limitation, and data minimization. While many organizations already have mature privacy programs, a fast-emerging trend is incorporating AdTech governance (and the digital advertising it facilitates) into the enterprise privacy program. Regulatory and consumer expectations now include a governed approach to tracking technologies.

Governance within this context is not one-size fits all. Privacy professionals should instead focus on creating an approach that is based on the following components: technology; policies and procedures; notices; and contracts and agreements.

Technology

□ Leverage key privacy technologies to scan, monitor, inventory, and categorize online trackers. These tools are becoming more widespread and can be found by using simple search terms like "cookie scanning" and "consent management" tools. For many organizations, this is a critical first step in surveying the landscape of trackers that exist across their organization's web properties. Organizations should regularly and consistently scan their web properties. Of course, only authorized online trackers should be deployed across your organization's web properties.

[29] *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 U.S. App. LEXIS 14951 (9th Cir. May 11, 2022).

Once your organization has sufficiently inventoried all trackers, the next step will be to do the following:

- ○ Ensure online tracking technologies, and especially social media pixels, are only deployed upon non-authenticated pages and are prohibited from being deployed on authenticated pages which require user login credentials.
- ○ Restrict vendor's use of data collected from website communications. This step supports the argument that vendors are not a third party.
- ○ Review the data flows to determine specifically how communications are being collected, where they are routed, how they are stored.

□ Ensure your consent management technologies are properly configured to align with your regulatory obligations and overall consent strategy.[30] This includes the use of tag managers, and a documented understanding of the data attributes that are collected by tracking technologies across your web properties.

□ Addition technical steps that organizations can take to reduce litigation risks include:

- ○ Obtain consent in the chatbot window to record the conversation.
- ○ Consider a pop-up or other notification when recording chatbot communications.
- ○ Route recordings to the website operator's servers.
- ○ Restrict the use of GET requests to duplicate communications.
- ○ Restrict/mask the data shared with third party cookies, pixels, and similar trackers.
- ○ Ensure that session replay tools only run on a small sample of website visitors, which should reduce the potential class size. This opens the door for a factual defense where plaintiffs are inaccurately alleging that everyone who visits the site have their sessions "recorded."

Policies and Procedures

□ Draft internal policies that clearly outline the roles, responsibilities, and expectations related to tracking technologies. This step is critical for defining and minimizing risk. Creating an established connection between legal and advertising teams is essential for ensuring that the individuals who are responsible for deploying tracking technologies are aware of their organization's risk posture. Of course, it is not enough to draft a policy and procedure based on regulatory requirements; appropriate stakeholders must be fully aware of their organization's policy vis-à-vis online trackers and understand how to implement these policies.

[30] Note that consent may be collected via a pop-up or banner notification for session replay cookies, pixels and similar technologies. However, this is not required by any law in the United States. While it may make your website a less attractive target of a lawsuit, the plaintiff's bar will likely look for other creative avenues for liability and is not a guaranteed shield against future claims.

Specifically, organizations must clearly outline their expectations regarding the use of online trackers in the form of a policy and accompanying standard operating procedure (SOP). SOPs should include a thorough and easy-to-understand process for managing and reviewing existing tracking technologies, as well as onboarding new ones and sunsetting those that are no longer to be used to marketing campaigns or for any other reasonable purpose. Onboarding should include risk management audit processes of any downstream parties on your websites.

Notices

- □ Draft privacy notices, including cookie consent disclosures, and establish a flexible process to update all public facing privacy/cookie notices, that aligns with your organization's inventory of online trackers. In drafting or revising notices, organizations need to determine their consent obligations. All privacy notices should include a detailed accounting of tracker usage, including the use of session replay cookies and similar technologies.

Contracts and Agreements

- □ Contracts should be used to ensure data access and use agreements are in place with authorized online trackers providers. Such agreements should clearly outline the data that authorized trackers may collect, and the purpose and use of the data are limited to the benefit of the company and not the authorized tracker. This may require limiting what data can be shared, sold, combined, or otherwise matched with other data points.

Appendix A – Wiretap Claims: Frequently Asked Questions

Key questions and answers surrounding the current wiretapping claims are included for convenience below.

1. What are typical wiretapping claims and who are the defendants?

The California Invasion of Privacy Act (CIPA) was enacted in 1967 to protect against wiretapping private conversations. While the text of CIPA focuses on telephone communications, courts have determined that CIPA applies to internet communications. CIPA regulates the following: (1) an unauthorized connection; (2) contents of a communication have been read/learned, (3) use of information has been obtained through wiretapping, and (4) aiding and abetting wiretapping. Courts generally apply the same analysis used to evaluate violations of the Federal Wiretap Act of 1968 (FWA) to determine whether CIPA has been violated.[31] The ubiquitous use of session replay cookies, chatbots, and pixel technologies sweeps in almost all companies as potential defendants. Defendants may include publishers and brands.

2. What should companies keep in mind when trying to navigate these claims?

Arguments for defending wiretapping claims are highly fact-specific and dependent on the technology at issue and disclosures made to website users. While there are a number of defenses, courts may split how to interpret them. For example, CIPA liability has been held to attach only to eavesdropping by a third party and not to recording by a participant to a conversation.[32] Thus, the defendant must either be a third party eavesdropper or a company that aids or assists that third party in violating CIPA. However, in California federal courts are split over whether a session replay provider is a third-party eavesdropper or a party to the communication.

3. What are the penalties for violating the state and federal wiretapping claims?

Violations of the FWA can incur damages of up to $10,000 per violation.[33] Fines for violating CIPA are $2,500 per violation.[34] Fines under similar state laws range from $1,000 to $50,000 per violation, depending on the state.

4. Is being found liable the only concern?

Lawsuits involving the session replay cookies, chat box, and pixel technologies are increasing. Companies may end up paying enormous settlements even if they do not go to trial.

[31] Saleh v. Nike, Inc., 562 F. Supp. 3d 503, 517 (C.D. Cal. 2021).

[32] Warden v. Kahn, 99 Cal. App. 3d 805, 811, 160 Cal. Rptr. 471 (1979) (finding that Section 631 "has been held to apply only to eavesdropping by a third party and not to recording by a participant to a conversation")

[33] 18 U.S.C. § 2520(c)(2) (2022)

[34] Cal. Pen. Code §631(a)

5. **What can should/companies who are concerned about wiretapping claims do?**

   In addition to the technical mitigation strategies listed in Appendix A above, companies should also: (1) update privacy policies to disclose the use of session replay cookies and similar technologies, (2) obtain consent in the chatbot window to record the conversation, (3) Restrict vendor's use of data collected from website communications to support an argument that the vendor is not a third party, and (4) review the data flows to determine specifically how communications are being collected, where they are routed, how they are stored.