AN A.S. PRATT PUBLICATION
JULY-AUGUST 2025
VOL. 11 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 6** **July-August 2025**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

California Court Rejects Attempt to Expand Third-Party Eavesdropping Claims to Internet Communications: How Your Business Can Mitigate Risk

By Catherine M. Contino and Usama Kahf*

In this article, the authors discuss a federal court decision dismissing a claim under California's Invasion of Privacy Act.

Businesses received some good news when a federal court recently dismissed a California Invasion of Privacy Act (CIPA) claim that aimed to expand the reach of the state's wiretapping law to cover internet communications. The order is the very first ruling to decide, on the merits, whether CIPA could support litigation over the issue of third-party website cookies since CIPA litigation exploded over the last three years.

The decision that granted summary judgment to the defendants keyed in on the fact that the third party's accessing of internet communications did not occur while the data was "in transit," but instead involved communications that had already taken place.

The big questions we are all asking now:

- How will this decision impact current CIPA litigation?
- Will we start to see the tide turn in businesses' favor?
- What can this decision teach you about risk mitigation of third-party technology you likely use on your website?

WHAT HAPPENED?

In *Torres v. Prudential Financial, Inc.*,[1] the court granted a motion for summary judgment filed by defendants (ActiveProspect, Prudential Financial, and Assurance IQ), which sought dismissal of plaintiffs' CIPA claim.

- 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 communication made

* The authors, attorneys with Fisher Phillips, may be contacted at ccontino@fisherphillips.com and ukahf@fisherphillips.com, respectively.

[1] Torres v. Prudential Financial, Inc., No. 22-cv-07465 (CRB) (N.D. Cal. Apr. 17, 2025).

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.[2]

- 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 alleged 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 alleged 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.

- In November 2024, a California federal court granted class certification to the claim in what appeared to be a first-of-its-kind decision.

WHAT IS A MOTION FOR SUMMARY JUDGMENT?

A motion for summary judgment is a request to the court to decide the case without a full trial. A party argues that there are no genuine disputes of fact in the case, and the law supports their side. This is typically filed after development of the record through discovery, including depositions.

THE DECISION IS A SOLID WIN FOR BUSINESSES

CIPA creates liability where a person willfully and without consent of all parties reads or attempts to read the contents of the communication while in transit. A participant to a conversation who uses a tape recorder to record a communication, even secretly, is not liable under CIPA.

- The court rejected defendants' first argument that ActiveProspect was a "participant" to the conversation. The court found that this software was not a party to a consumer's communications on Prudential's website through its online form. It cited evidence in the record that demonstrated employees of the software company could view session replays (despite evidence that such access was for customer support purposes). Therefore, the software did not function as a mere "tape recorder."

- However, the court found that ActiveProspect did not read or attempt to read the contents of individuals' communications with the Prudential website while in transit. The court found that even if the third-party software intercepted the contents of individuals communications with the

[2] Javier v. Assurance IQ, LLC, No. 21-16351 (9th Cir. May 31, 2022).

website, there was no evidence that the third party reads or tries to read the contents of the communication while it is in transit. Although the court acknowledged that CIPA was meant to be interpreted broadly to include new technology, the plaintiffs' requested interpretation went too far.

- Allowing this claim to proceed without any evidence that the communications were read in transit, or because ActiveProspect "could have" learned of the contents "would stretch CIPA's statutory language too far to interpret 'while . . . in transit' to encompass any hypothetical future attempt to read or understand the meaning of a communication."

- Without any evidence that ActiveProspect "independently attempted to decipher the contents of any communication," the court rejected plaintiffs' CIPA claim.

IMPACT OF DECISION

This decision demonstrates the court's restraint in broadly applying CIPA's wiretapping prohibition to internet communications. The court outlines what a plaintiff needs to prove to be successful on these claims, which can assist businesses in mitigating potential risk when utilizing this type of technology.

While the plaintiffs in this case still have one cause of action left (Invasion of Privacy under the California Constitution), their potential damages are much more limited. By granting summary judgment on the CIPA claim, the court ensured that the plaintiffs will lose out on the chance to recover statutory damages of $5,000 per violation – which represented the most valuable part of their claims.

WHAT CAN YOUR BUSINESS DO TO MITIGATE RISK?

With legal theories under CIPA continuing to expand, businesses operating websites must closely examine online data collection and sharing practices. To mitigate the growing risks, companies should consider taking the following steps:

- *Understand How Third Parties Are Using Your Data*

If you use third-party software on your website, understand how those entities are collecting, storing, and sharing data, allowing for proactive compliance strategies. Conduct regular data mapping exercises to understand exactly how data is captured, used, and stored. Take steps to ensure that the third parties do not attempt to read or access the contents of transmissions of data between the user and your website while the user is interacting with the website. Accessing the contents of such transmissions after the end of the user session may present other legal risks to consider, but at least you would be able to document how third parties do not view the data while the communication is in transit.

- *Consider Your Consumer-Facing Policies*

Review and revise consumer facing policies to include clear provisions on data collection, user consent, and dispute resolution.

- *Notice and Disclosure:* Review and revise online privacy policies and terms of use to explicitly inform users about the collection and sharing of search term data collected through website search boxes.
- *Class Action Waivers*: Help mitigate potential legal exposure and control litigation risk by incorporating class action waivers into terms of use.
- *Dispute Resolution*: Include specific dispute resolution procedures, such as mandatory arbitration, to further protect against litigation risks.

CONCLUSION

Companies should closely monitor new and progressing privacy litigation claims to stay ahead of legal risk. Understanding litigation trends can help companies plan proactive measures that balance online business needs and consumer privacy expectations.