AN A.S. PRATT PUBLICATION
MAY 2025
VOL. 11 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 4** **May 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.

Massachusetts Supreme Court Takes a Closer Look at Wiretap Laws, Potentially Narrowing Privacy Actions

By John T. Wolak and Ravipal Singh*

In this article, the authors review a recent decision by the highest court in Massachusetts addressing whether tracking a user's activities on a website and sharing that data with third parties constitutes intercepting communications in violation of Massachusetts' 1968 Wiretap Act.

The Massachusetts Supreme Judicial Court recently issued an important ruling in *Vita v. New England Baptist Hospital et al.*[1] addressing whether tracking a user's activities on a website and sharing that data with third parties constitutes intercepting communications in violation of Massachusetts' 1968 Wiretap Act (the Act).

In dismissing the plaintiff's statutory claims, the court emphasized that it is the responsibility of the legislature – and not the court – to address gaps in statutory protections related to privacy and modern tracking technologies, highlighting that as technology and any corresponding digital privacy concerns evolve, legislative frameworks must be modified to adapt accordingly.

THE CASE

Plaintiff Kathleen Vita claimed that New England Baptist Hospital and Beth Israel Deaconess Medical Center violated the Act by "intercepting" communications without her consent or knowledge through the use of tracking tools on their websites. Specifically, the plaintiff alleged that the hospitals used third-party software to record her activity when she browsed the hospitals' websites to obtain information about doctors, search for information about medical symptoms and other healthcare-related issues, and obtain and review medical records.

The plaintiff alleged that the hospitals then shared this data with third parties that processed the data for targeted advertising campaigns tailored to the individual user's data. The court concluded that although the web tracking practices raised valid privacy concerns, these issues fell outside the scope of the Act, which was enacted to prohibit secret electronic eavesdropping on person-to-person conversations or messaging. In reaching this conclusion, the court found that the term "communication" in the Act was ambiguous as applied to the plaintiff's interactions with the websites, and the Act's

* The authors, attorneys with Gibbons P.C., may be contacted at jwolak@gibbonslaw.com and rsingh@gibbonslaw.com, respectively.

[1] Vita v. New England Baptist Hospital et al. (Mass. Oct. 24, 2024).

legislative history did not provide a basis for extending the scope of the Act beyond person-to-person communications, such as to encompass a person's interaction with a website. Thus, the court dismissed the plaintiff's claims for violation of the Act.

This ruling highlights how interpretations of the term "communication" can lead to diverging outcomes in wiretap cases. For example, California's Invasion of Privacy Act (CIPA) specifically prohibits the intentional interception or recording of any "confidential communication" without the consent of all parties involved, and California courts have interpreted "communication" more expansively to include digital interactions. Unlike the Massachusetts Act, which was narrowly focused on traditional, person-to-person communications, the CIPA has been applied to protect one-way recordings[2] and internet communications.[3]

It is important to note that the court also rejected the hospitals' claim that the plaintiff and other website users had actual knowledge of the data collection and sharing practices through disclosures found in the website cookie banner and privacy policy.

Specifically, the hospitals claimed that they had disclosed the use of third-party tracking technology and third-party data sharing by various express disclosures, including "We and our Third Party Service Provider collect and save the default information customarily logged by worldwide web server software."

After briefly reviewing these disclosures, both the majority and the dissenting opinions determined that the hospitals' disclosure of website data collection and sharing practices was misleading, did not adequately reveal the extent of third-party tracking, and concealed the targeted advertising arrangements with third parties.

CONCLUSION

The Massachusetts Supreme Court's ruling reinforces the limitations of legacy privacy laws in addressing new technologies and serves as a critical reminder that as digital privacy concerns evolve, so too must the legislative framework. The court's opinion also emphasizes the importance of accurate and complete disclosures in privacy notifications and cookie banners; although not definitive shields against legal action, accurate and complete disclosures can play a helpful role for a defendant against allegations of improper tracking, collection, and sharing of user data.

[2] Gruber v. Yelp Inc., 55 Cal.App.5th 591 (Cal. Ct. App. 2020).

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