AN A.S. PRATT PUBLICATION
OCTOBER 2025
VOL. 11 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 8** **October 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.

Neural Data Privacy Regulation: What Laws Exist and What Is Anticipated?

By Kristina Iliopoulos and Nancy Perkins*

In 2024, Colorado and California enacted the first U.S. state privacy laws governing neural data, and at least six other states are following suit in an attempt to increase privacy protections applicable to the use of neurotechnology. The authors of this article discuss the technology, the privacy concerns, the enacted and proposed laws and proactive data governance.

Legislators at both the federal and state levels are taking steps to regulate the collection, use, and disclosure of neural data. In 2024, Colorado and California enacted the first U.S. state privacy laws governing neural data, and at least six other states are following suit in an attempt to increase privacy protections applicable to the use of neurotechnology.

Neurotechnology encompasses a broad range of devices that track brainwaves, including medical devices, consumer products (including some wearable devices, virtual reality systems, and even some smartphone applications), and invasive devices. Such technology has shown promising benefits, such as treating paralysis and predicting seizures. However, lawmakers have expressed concern regarding data misuse and even "brain-control weaponry" on the extreme end. The actions legislators and regulators take based on these concerns will have a significant impact on a variety of different types of companies that collect neural data, including Elon Musk's NeuraLink, Blackrock Neurotech, Neurable, and Neurode.

KEY PRIVACY CONCERNS

Concerns about neurotechnology and its regulation have developed almost as quickly as the technology itself. The Neurorights Foundation released a report[1] in April 2024, highlighting gaps in consumer neurotechnology device companies' privacy practices. The report found that nearly every company reviewed appeared "to have access to the consumer's neural data and provide no meaningful limitations to this access."

State and federal lawmakers have similarly raised concerns about data misuse associated with neurotechnology. In April 2025, several U.S. senators urged[2] the U.S. Federal Trade Commission (FTC) to take action to protect American's neural data from

* The authors are attorneys at Arnold & Porter Kaye Scholer LLP. They may be contacted at kristina.iliopoulos@arnoldporter.com and nancy.perkins@arnoldporter.com, respectively.

[1] https://perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf.

[2] https://www.commerce.senate.gov/2025/4/cantwell-schumer-markey-call-on-ftc-to-protect-consumers-neural-data.

"potential exploitation or sale, as brain-computer interface (BCI) technologies rapidly advance." The senators noted that "unlike other personal data, neural data – captured directly from the human brain – can reveal mental health conditions, emotional states, and cognitive patterns, even when anonymized." The FTC could potentially use its authority to discipline unfair and deceptive practices to address these concerns, but it has not responded to the letter or otherwise expressed its intent in this regard.

Currently, most U.S. federal and state privacy laws provide minimal protection for neural data. For example, the Health Insurance Portability and Accountability Act (HIPAA), while expansive in defining "health" information, protects neural data only to the extent that it is received or created by HIPAA "covered entities," i.e., health plans, certain health care providers, "health care clearinghouses"; or business associates of covered entities. Similarly, although many state consumer privacy laws apply to "sensitive personal information," neural data is not clearly included in the state law definitions of that term.

As California and Colorado have determined, privacy legislation specific to neural data or amendments to existing privacy law may be critical to protect individuals from misuses of neural data. But those two states have not approached their regulation of neural data in quite the same way, and the proposals of other states indicate that, absent federal legislation (which Congress is highly unlikely to pass in the near future), the laws governing neural data will develop inconsistently across the states. Determining how to plan for compliance may therefore be an ongoing challenge.

CALIFORNIA AND COLORADO ENACTMENTS

As noted, California and Colorado are currently the only states with enacted neural data-focused laws. Colorado was the first state to explicitly extend privacy rights to neural data by expanding the definition of "sensitive data" in the state's existing consumer privacy law[3] to include "neural data." Under the Colorado law, regulated entities must obtain consent before collecting or processing "sensitive data," so such consent is now required to obtain, use, or disclose neural data; and other protections for "sensitive data" apply as well. Similarly, the California legislature amended the California Consumer Privacy Act (CCPA) to expressly include neural data in the definition of "sensitive personal information," thereby granting consumers special rights with respect to their neural data.

California and Colorado's definitions and treatment of "neural data," however, are not uniform. Colorado's law defines "neural data" as "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device." The CCPA, in contrast,

[3] Colo. Rev. Stat. Ann. § 6-1-1303.

defines "neural data" to exclude any data that is inferred from nonneural information – which means that behavioral and physiological data that could be used to infer a mental state is not "sensitive personal information" under the CCPA. For example, wearable devices that capture heart rate, which is data from the circulatory system, not the central or peripheral nervous system, would not be "sensitive personal information" under the CCPA (even though that data could be used to reveal stress levels), while electrical activity data from consumer neurotechnologies (devices that directly capture data from the brain) would.

There is also asymmetry between California and Colorado's requirements for obtaining consent to process neural (and other sensitive personal) data. Colorado's law requires regulated businesses to obtain opt-in consent to collect and use neural data. In comparison, the CCPA only affords consumers a limited right to opt out of the use and disclosure of their neural data, and then only if the use or disclosure is for purposes other than to provide goods or services requested by the consumer. Conversely, the CCPA has a broader reach in defining "consumer" to include employees and individuals acting in a business-to-business context, whereas the Colorado law defines "consumer" to exclude employees and business representatives.

PROPOSED STATE MEASURES – HIGHLIGHTS

In addition to amending the CCPA to address neural data specifically, the California legislature is considering a bill[4] that would require a covered business to use neural data only for the purpose for which the neural data was collected and to delete neural data when the purpose for which the neural data was collected is accomplished. The bill would define a "covered business" to mean a person or entity that makes available a brain-computer interface to a person in the state and "brain-computer interface" to mean a system that allows direct communication and control between a person's brain and an external device.

The other states in which neural data privacy legislation is pending include Connecticut, Illinois, Massachusetts, Minnesota, Montana and Vermont. Those states' proposals vary in scope and substance, as indicated briefly below.

Connecticut's bill[5] would amend the state's privacy law to include neural data as a type of sensitive data. The definition of "neural data" is broader than Colorado's definition – it is not limited to data used for identification purposes. Connecticut's bill would require an opt-in consent before processing neural data and data impact assessments for each processing activity.

Illinois' bill[6] would amend the Illinois Biometric Information Privacy Act to include neural data as a "biometric identifier," requiring entities to provide individuals with

---

[4] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB44.

[5] https://www.cga.ct.gov/2025/TOB/S/PDF/2025SB-01356-R00-SB.PDF.

[6] https://www.ilga.gov/Legislation/BillStatus.
FullText?GAID=18&DocNum=2984&DocTypeID=HB&LegId=161234&SessionID=114.

notice regarding how neural data is collected and stored, and obtain express written consent before such collection.

In Massachusetts, a state without a comprehensive consumer privacy law, legislators have proposed the Neural Data Privacy Protection Act,[7] which, like the amended CCPA, would provide protections for neural data but omit from such protection information inferred from non-neural data. Under the Massachusetts bill, covered entities would be prohibited from (1) collecting or processing neural data unless it is strictly necessary to provide or maintain a product or service; (2) transferring neural data to a third party without consent or other limited exceptions; or (3) processing neural data for targeted advertising.

Minnesota's proposal[8] is a standalone bill providing separate protections for neural data and mental privacy, and would apply to both private and governmental entities. The bill would prohibit governmental entities from collected data transcribed from brain activity without informed consent and would prohibit companies from using a brain-computer interface to bypass conscious decision-making by an individual.

Montana's bill[9] would extend existing genetic information privacy safeguards to neurotechnology data and would give state residents more control over their neural data.

Vermont's bill[10] aims to prohibit brain-computer interfaces from bypassing conscious decision-making without consent.

PROACTIVE DATA GOVERNANCE

Given the inconsistency in scope and substantive requirements among the newly enacted and proposed neural data privacy laws, entities that deal with neural data face something of a moving target in seeking to design their products and activities to comply with such laws. Applying fundamental privacy protection principles and considering comparative regulatory approaches to other types of personal information, such as genetic information and biometric information, may serve as helpful elements of a neural data privacy protection framework.

A basic data governance protocol should include a model and roadmap that aligns with a company's mission and tolerance for risk. A process for monitoring compliance with the company's model against requirements and best practices should be implemented.

---

[7] https://malegislature.gov/Bills/194/HD4127.

[8] https://www.revisor.mn.gov/bills/text.php?number=SF1240&version=latest&session=ls94&session_year=2025&session_number=0&format=pdf.

[9] https://bills.legmt.gov/#/laws/bill/2/LC0005?open_tab=bill.

[10] https://legislature.vermont.gov/Documents/2026/Docs/BILLS/H-0366/H-0366%20As%20Introduced.pdf.

Finally, internal policies should explain how neural data is collected, stored, shared, and secured. This policy should be regularly reviewed against any newly enacted laws to ensure continued compliance.

Companies should also keep in mind that, because privacy laws directed toward neural data are in their infancy and there are likely to be more coming, they could very well play a role in shaping the direction of these laws through direct lobbying or participating in trade associations devoted to lobbying.