Wolters Kluwer

Strategic Perspectives | Cybersecurity Policy Report

Rethinking Privacy of the Mind: Why Protecting Neural Data Is Insufficient

by Daniel J. Solove, Bernard Professor of Intellectual Property and Technology Law at the George Washington University Law School

Today, data is being gathered and analyzed about people at an unprecedented scale, but there has been one area that has remained a refuge—the hidden depths of the mind. In the 1998 movie, *The Truman Show,* a person named Truman Burbank discovers he has had his life filmed 24/7 for a reality TV show. At the end, he finally speaks to the show's director, who tells him that he has been watching him his entire life. Truman replies: "You never had a camera in my head!"

Now, almost thirty years later, *The Truman Show* remains quite prescient. But we're quickly approaching the time when there may be ways to look inside people's heads. Technologies can now read the electrical activity in the brain and can even communicate with the brain to enable people to control software or devices with their minds.

As these new technologies emerge, legislatures have acted quickly to address privacy concerns. But these efforts are incomplete if the goal is to protect privacy of the mind because neural data is part of a broader constellation of data that relates to our mental activity.

Neural data is necessary to protect privacy of the mind but is far from sufficient. In many cases, there might be other data we want to protect more than neural data. In today's age of AI and Big Data, so much about our mental activity can be learned from gathering and analyzing non-neural data. To truly protect privacy of the mind, the law must radically rethink its approach to how it regulates the collection and processing of personal data. But how?

Neural Data and the Law

In the past few years, several states have attempted to provide privacy protections to neural data, most by amending existing laws to add neural data as a type of sensitive data (California, Colorado, Connecticut, and Delaware). In 2026, Vermont passed a consumer privacy law which includes neural data among its categories of sensitive data.

The laws have different definitions of neural data.

- California Consumer Privacy Act (CCPA): "information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information."[1]
- Colorado Privacy Act: "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."[2]
- Connecticut Act Concerning Personal Data Privacy and Online Monitoring: "any information that is generated by measuring the activity of an individual's central nervous system."[3]
- Delaware Personal Data Privacy Act: "data that is generated by measuring the activity of an individual's central nervous system."[4]
- Vermont Data Privacy and Online Surveillance Act: data "generated by measuring the activity of an individual's central nervous system."[5]

Montana amended its Genetic Information Privacy Act to include "neurotechnology data" (rather than neural data). This law only applies to genetic testing or products or the analysis of genetic data. GIPA defines "neurotechnology data" as "information that is captured by neurotechnologies, is generated by measuring the activity of an individual's

1 Cal Civ. Code § 1798.140 (ae)(1)(G)(ii) (West 2026).
2 Colo. Rev. Stat. Ann. § 6-1-1303(16.7) (West 2025).
3 Conn. Gen. Stat. Ann. § 42-515(24), (39) (West 2026).
4 6 Del. C. § 12D-102(e).
5 Vt. Stat. Ann. tit. 9, § 2415a(31) (2026).

© 2026 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

central or peripheral nervous systems, or is data associated with neural activity, which means the activity of the neurons or glial cells in the central or peripheral nervous system, and that is nonneural information."[6]

At the federal level, Senator Schumer introduced the MIND Act in 2025, which would require the FTC to study issues involving neural data. It defines neural data as "information obtained by measuring the activity of an individual's central or peripheral nervous system through the use of neurotechnology."[7]

The laws share many similarities in their definitions, but there are some differences, the main one being whether neural data extends just to the central nervous system (CNS) or also to the peripheral nervous system (PNS). The CNS involves the brain and spinal cord (the "command center") and the PNS involves "all the cranial and spinal nerves that branch off from the CNS to the rest of the body" and send "relay messages" from the CNS.[8] California, Colorado, and Vermont's definitions include both CNS and PNS while Connecticut, Delaware, and Montana only cover CNS.[9]

Does Categorizing Neural Data as Sensitive Provide Enough Protection?

Most laws merely add neural data as a category of sensitive data, but the heightened protections for sensitive data are only somewhat more protective. For sensitive data, most laws require opt-in consent rather than opt-out as well as a privacy impact assessment. But these protections don't go far enough.

Privacy impact assessments (PIA) are an essential tool to protecting privacy, for it's hard to address risks without first identifying them. In most laws, however, the PIA requirement is not particularly rigorous. The laws fail to ensure that PIAs are thorough and that the risks are properly addressed. There often is no meaningful accountability.

Opt-in consent is harder to obtain than opt-out (which is a joke), but it's still easy to obtain an opt-in – just add an accept button. Opt-in fails to guarantee that people actually understand what they're agreeing to or even that they have the foggiest notion about it.[10]

For example, consider the Black Mirror TV series episode "Common People" (2025), where a woman facing a terminal brain injury has the damaged part of her brain removed and replaced by an artificial component. The technology works as a service which requires a subscription fee. Over time, the company increases the fee and downgrades the service, creating various tiers. People who aren't in the top tiers suddenly start speaking ads from advertisers. As it goes on, the episode grows darker by the minute.

Sensitive data protections in existing privacy law would do little to address the situation in "Common People." There was purported agreement to the terms of service. Instead of providing protection, opt-in just enabled the company to do what it did.

Categorizing neural data as sensitive has little effect on government access. In many cases, the government can readily access much sensitive data without any oversight or restriction. Even when the data is obtained by a warrant, the protection is weak.[11] According to one study, "Ninety-eight percent of warrant reviews eventually result in an approval, and over 93% are approved on first submission. . . . [T]he median time for review is only three minutes."[12] If the government wants to access data about our minds, it can and will under existing law.

Protecting Privacy of the Mind Goes Beyond Merely Protecting Neural Data

Laws protecting neural data were inspired by broader concerns about privacy of the mind. For example, the Colorado legislature declared in its findings that neural data is "extremely sensitive and can reveal intimate information about individuals, including

6 Mont. Code. Ann. § 30-23-102 (10)(a).

7 *S.2925 - MIND Act of 2025*, Congress.Gov, https://www.congress.gov/bill/119th-congress/senate-bill/2925/text/is (last visited Aug. 16, 2026).

8 Olivia Guy-Evans, "Central Nervous System Vs. Peripheral Nervous System," Simply Psychology (June 25, 2025), https://www.simplypsychology.org/central-nervous-system-vs-peripheral-nervous-system.html.

9 Jameson Spivack and Chris Victory, *The "Neural Data" Goldilocks Problem: Defining "Neural Data" in U.S. State Privacy Laws*, Future of Privacy Forum (June 27, 2026), https://fpf.org/blog/the-neural-data-goldilocks-problem-defining-neural-data-in-u-s-state-privacy-laws/.

10 Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law,* 104 B.U. L. Rev. 593 (2024), https://ssrn.com/abstract=4333743.

11 Andrew Guthrie Ferguson, Your Data Can Be Used Against You (2026).

12 Miguel de Figueiredo, Brett Hashimoto, and Dane Thorley, *Unwarranted Warrants? An Empirical Analysis of Judicial Review in Search and Seizure*, 138 Harv. L. Rev. 1959 (2025).

© 2026 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

information about health, mental states, emotion, and cognitive functioning."[13]

What I'm referring to as privacy of the mind is similar to Professor Nita Farahany's concept of the "right to cognitive liberty." In her book, *The Battle for Your Brain,* she argues that the law must protect a right to cognitive liberty which consists of a "bundle of rights" that include "mental privacy, freedom of thought, and self-determination."[14]

I generally agree with Farahany. Her view of privacy is narrower than my conception. For Farahany, "cognitive liberty" is the umbrella concept under which privacy is a subset, involving limiting the collection and processing of data about our mental activities. I view privacy as a larger umbrella that encompasses the same things that Farahany classifies under cognitive liberty.[15]

In this essay, I'll use the term "privacy of the mind." To be meaningful, the protection of privacy of the mind must involve protection of people's mental activity, thoughts, beliefs, and emotions against at least two things: (1) unwarranted invasive probing; and (2) manipulation (undue influence). These two goals seem quite uncontroversial; the difficulty is figuring out how the law should achieve them.

The Difficulties of Singling Out Types of Data

A major problem with attempts to protect privacy of the mind is that it is incredibly difficult to single out types of data. Most of the time, efforts to do so will fail quite miserably. This fact greatly complicates efforts to protect privacy of the mind by singling out neural data.

The Central and Peripheral Nervous System Distinction Is Blurry and Wrongheaded

As I discussed above, many laws distinguish between CNS and PNS in their neural data definitions, with some laws only protecting data from the CNS. None of the laws explicitly articulate the difference between CNS and PNS. As Jameson Spivack and Chris Victory note, covering only central nervous system data "may be difficult to implement because it's not clear that it's possible to truly separate the data from these two systems, as they are interlinked."[16]

Data about the CNS can be inferred from PNS data. The CNS and PNS are deeply interconnected, for they are part of the entire nervous system.

Neural Data Isn't All the Same

Farahany notes that it's far too simplistic to assume that neural data is the most intimate and revealing data about mental activity:

> [W]e should recognize that not all neural data is equally sensitive. While the right to mental privacy should protect the entire spectrum of neural data—identifying, automatic, memorialized, and silent utterances—the individual interest in mental privacy should be the most unyielding when silently uttered or memorialized information is sought. When automatic brain functioning or identifying information is sought instead, mental privacy may at times yield to societal interests.[17]

Farahany is correct that the law shouldn't protect all neural data in the same way because it does not all have the same sensitivity. The tricky part is how to figure out what is most sensitive, and this matter doesn't primarily involve the type of data; it involves the use of the data.

Intellectual and Emotional

Mental activity involves both intellectual thoughts and beliefs as well as emotions and desires. It also involves many unconscious processes, for the brain operates the body mostly automatically. To protect privacy of the mind, the law must protect all of these things.

Professor Neil Richards argues that one of the most important dimensions of privacy the law should protect is "intellectual privacy," which he defines as the ability "to develop ideas and beliefs away from the unwanted gaze or interference of others."[18] Intellectual privacy, he argues, requires "protection from surveillance or interference when we are engaged in the process of generating ideas—thinking, reading, and speaking with confidants before our ideas are ready for public consumption."[19] The law "must safeguard the processes of intellectual explorations and belief

13 2024 Colo. Legis. Serv. Ch. 68 *Id.* § 1(2)(d).

14 Nita A. Farahany, The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology 11 (2023).

15 I view the concept of privacy as a plurality of different but related things. Daniel J. Solove, Understanding Privacy (2008).

16 Spivack and Victory, *supra.*

17 Farahany, Battle for Your Brain, 33.

18 Neil M. Richards, *Intellectual Privacy,* 87 Tex. L. Rev. 387, 389 (2008).

19 Neil M. Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age 5 (2015).

© 2026 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

formation" to protect "our ability to make up our minds freely."[20]

Professor Danielle Citron argues that it is also essential for the law to protect "intimate privacy," which she defines as "the extent to which others have access to and information about, our bodies and minds (thoughts, desires, and fantasies); health; sex, sexual orientation, and gender; and close relationships."[21] This too involves the mind—our feelings and desires.

Intellectual privacy and intimate privacy are dimensions of privacy of the mind, and these dimensions extend far beyond neural data.

Mind and Body

Discussions of privacy of the mind must be careful to avoid assuming a strict Cartesian division between mind and body. The mind and the body work together and are deeply interconnected. The body gives many clues to mental activity, such as heart rate and eye movements.[22]

Despite the popularity today of the metaphor of the brain as a computer, the brain is not merely a computer.[23] The brain is more than just a data processing machine, and it can't be neatly separated into a hardware and software component. Chemicals are a key part of mental functioning, and the same chemicals that regulate mood also regulate bodily functions like digestion and blood pressure.

If the goal is to protect the privacy of what we're thinking and feeling in a meaningful way, focusing merely on neural data is woefully inadequate. Neural data can reveal love or arousal, but so can bodily data. Neural data is linked to thoughts, but so is what we say, read, and do.

Privacy of the Mind Can't Be Protected in Isolation

In the end, privacy of the mind can't be protected in a neural silo. Our minds are involved in nearly everything we do, and everything we do, in turn, can give rise to inferences about the goings on in our minds. We can't protect privacy of the mind just by focusing on the mind alone.

Manipulation

Another dimension of privacy of the mind (or cognitive liberty) is protection against manipulation. When the use of data or certain techniques to shape behavior becomes too manipulative, it starts down a road toward mind control. The difficulty is that there is a spectrum of influence, from acceptable means of persuasion to more dicey manipulative techniques to more controlling and problematic ones.

It's hard to draw a line or concoct a simple test to know where to draw the line. A robust body of literature explores when this line is crossed. Some argue that manipulation occurs when it "deprives individuals of their agency by distorting and perverting the way in which individuals typically make decisions"[24] or when it involves "an intentional attempt to influence a subject's behavior by exploiting a bias or vulnerability."[25]

Unfortunately, the law barely addresses the manipulation of people with digital technologies, except sometimes with dark patterns. To truly protect privacy of the mind, however, the law must address this issue.

To add further complication, most manipulation occurs without neural data. Based on studies by Daniel Kahneman, Amos Tversky, and others, it is well known today that there are systematic biases and heuristics in the way people think.[26] People's thinking and behavior can readily be manipulated by framing, which can be highly targeted and personalized based on profiling. This is how Cambridge Analytica targeted different versions of political ads to people to enhance their effectiveness. Digital technologies can weaponize all that is known about the way people think, decide, and behave to dramatically shape them. To tackle

20 *Id.* at 5, 96.

21 Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age xii (2022).

22 Patrick Magee, Marcello Ienca, & Nita Farahany, *Beyond neural data: Cognitive biometrics and mental privacy,* 112 Neuron 3017, 3021 (2024).

23 Matthew Cobb, Why Your Brain is Not a Computer, THE GUARDIAN, https://theguardian.com/science/2020/feb/27/why-your-brain-is-not-a-computer-neuroscience-neural-networks-consciousness. Robert Epstein, "The Empty Brain," Aeon (May 18, 2016), https://aeon.co/essays/your-brain-does-not-process-information-and-it-is-not-a-computer.

24 Ido Kilovaty, *Legally Cognizable Manipulation,* 34 Berkeley Tech. L.J. 449, 469 (2019).

25 Shaun Spencer, *The Problem of Online Manipulation,* 2020 U. Ill. L. Rev. 959, 990 (2020). For more on manipulation, see Daniel Susser, Beate Roessler, and Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World,* 4 Geo. L. Tech. Rev. 1 (2019); Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995 (2014).

26 Daniel Kahneman, Thinking Fast and Slow (2011).

© 2026 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

manipulation, the law must protect far more than neural data.

Thinking Beyond the Mind

How do we protect privacy of the mind in a meaningful and complete way? Line drawing is exceedingly difficult. Singling out types of data, such as neural data, is incomplete and not workable in many situations.

Ironically, the best way to protect privacy of the mind is to start thinking beyond just the mind. Privacy of the mind can be meaningfully protected through broader protection of the body and everything we do.

Key Takeaways

1. Recent privacy laws are attempting to protect neural data as a way to protect privacy of the mind.
2. The laws define neural data in different ways, with the most notable difference being that some laws define it as only involving data measuring the central nervous system (CNS) while others also include the peripheral nervous system (PNS).
3. Many laws are protecting neural data by classifying it as a form of sensitive data in their consumer privacy laws.
4. Not all neural data is equally sensitive.
5. The CNS/PNS distinction breaks down because PNS data can be highly revealing of mental activity.
6. Focusing on neural data is necessary but not sufficient to protect privacy of the mind. Inferences about mental activity can be made from many other types of personal data.
7. Policymakers will likely continue to make attempts to protect privacy of the mind, and these attempts might eventually extend beyond narrow and limited protections of neural data.

Daniel J. Solove is the Bernard Professor of Intellectual Property and Technology Law at the George Washington University Law School. He is the founder of TeachPrivacy, a company that provides workforce privacy, cybersecurity, and AI training to companies and organizations around the world. He is the author of 10+ books and 100+ articles. You can follow his events, writings, training, cartoons, and resources by subscribing to his free weekly newsletter.

© 2026 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.