

5-2023

The Constitutionality of Brain Searches

Wayne Unger

Follow this and additional works at: https://repository.uclawsf.edu/hastings_constitutional_law_quarterly



Part of the [Constitutional Law Commons](#)

Recommended Citation

Wayne Unger, *The Constitutionality of Brain Searches*, 50 HASTINGS CONST. L.Q. 321 (2023).

Available at: https://repository.uclawsf.edu/hastings_constitutional_law_quarterly/vol50/iss4/2

This Article is brought to you for free and open access by the Law Journals at UC Law SF Scholarship Repository. It has been accepted for inclusion in Hastings Constitutional Law Quarterly by an authorized editor of UC Law SF Scholarship Repository. For more information, please contact wangangela@uchastings.edu.

The Constitutionality of Brain Searches

BY WAYNE UNGER*

Abstract

If technology could read your mind and capture your thoughts as storable and processable data, would that frighten you? Recent advancements in brain-computer interfaces will likely make mind-reading a reality, and if it does, it presents the last stand or final frontier in the battle for privacy protections. It is well established that an individual must be able to retreat into their home and be free from government intrusion. But if an individual cannot retreat into their own mind free from government intrusion, then true solitude will become extinct. In a future state where brain-computer interfaces can actively decode an individual's ideas, thoughts, and beliefs—neurodata—what constitutional protections, if any, exist to preclude government intrusion and protect the freedom of thought?

This Essay analyzes Fourth Amendment jurisprudence as applied to neurodata. More specifically, it examines the Court's current perspectives regarding highly sensitive and intimate data to neurodata, and in doing so, it utilizes Matthew Tokson's emerging principles of Fourth Amendment privacy. I argue that neurodata unequivocally falls within the Fourth Amendment's protections, and I provide a normative justification for extending the Fourth Amendment to this emerging technology and category of data.

* Visiting Assistant Professor of Law, Gonzaga University School of Law. Fellow, Center for Law, Ethics, and Commerce, Gonzaga University School of Law. Thanks to the following individuals for feedback and comments related to the subject matter of this Essay: Nita Farahany; Emily Murphy; Agnieszka McPeak; Mary Pat Treuthart; Dr. Diana Bowman; Dr. K Royal; the faculties at Gonzaga University School of Law, Quinnipiac University School of Law, Seattle University School of Law, University of Idaho College of Law, and Capital University School of Law; and the participants at the 2022 Governance of Emerging Technologies and Science (GETS) Conference at Arizona State University's College of Law. In addition, many thanks to my research assistants, Carly Roberts, Gunnar Peterson, and Nate Sargent. Special thanks to my faculty assistant, Nancy Moss.

TABLE OF CONTENTS

Introduction	322
I. Neurodata-Capturing Technologies & Fourth Amendment Searches of the Brain	325
II. Unreasonable Searches of Intimate Data	327
A. The Reasonable Expectation of Privacy Test.....	328
B. Is it a search?.....	329
C. Was It Reasonable?	333
III. The Normative Justification for Extending Fourth Amendment Protection to Neurodata	341
A. The Origins of the Fourth Amendment Principles	341
B. Moral Reasoning	344
Conclusion.....	347

Introduction

Even before the country’s founding, colonists recognized an inalienable right to the freedom of thought. Since the ratification of the Bill of Rights, courts and scholars have read the freedom of thought into the First Amendment.¹ Although the freedom of thought is not explicitly stated in the First Amendment, the express liberties of this Amendment are inherently intertwined with the freedom of thought and belief. Without the freedoms of speech and expression, as Justice Frankfurter proclaimed, “thought becomes checked and atrophied.”² Moreover, the widely recognized First Amendment’s marketplace of ideas theory, first asserted by Justice Holmes in *Abrams v. United States*,³ generally supports the free trade of ideas. As he stated in that case, “the ultimate good desired is better reached by [the] free trade of ideas—that the best test of truth is . . . to get itself accepted in the competition of the market.”⁴

1. See, e.g., *Palko v. Connecticut*, 302 U.S. 326 (1937) (overruled in *Benton v. Maryland*, 395 U.S. 784 (1969), on other grounds) (stating “[The] freedom[s] of thought, and speech. Of [these] freedom one may say that it is the matrix, the indispensable condition, of nearly every other form of freedom.”).

2. *Kovacs v. Cooper*, 336 U.S. 77, 94 (1949) (Frankfurter, J., concurring); see generally Lucas Swaine, *Freedom of Thought as a Basic Liberty*, 46 POL. THEORY 405, 414 (2018) (arguing that the freedom of thought is closely related to the freedom of expression, but also noting that the freedom of thought is distinct because the “central reason [for the difference] is that one can think a wide variety of thoughts without ever expressing them. People are capable of thinking things that they do not disclose to others.”); Wayne Unger, *Stay Out of My Head: Neurodata, Privacy, and the First Amendment*, WASH. & LEE. L. REV (forthcoming 2023).

3. *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

4. *Id.*

In his First Amendment scholarship, Professor Neil Richards furthers the general principle that the freedom of thought is coupled with the freedoms of speech and expression. He asserts that the First Amendment requires intellectual privacy, which he describes as a “zone of protection that guards our ability to make up our minds freely.”⁵ Here, the freedom to contemplate allows us to think about existing ideas and to imagine new ones.⁶

Elsewhere, I have argued that Neil Richard’s theory of intellectual privacy is about the *production* of ideas, thoughts, and beliefs.⁷ I posited that the First Amendment also guards against governmental *access* to one’s ideas and thoughts.⁸ The production and access protections of the First Amendment join the well-established recognition that the First Amendment protects the *presentation* of ideas, thoughts, and beliefs.⁹ In *Watchtower Bible & Tract Society of New York, Inc. v. Village of Stratton*, the Supreme Court recognized that the First Amendment prohibits licensing schemes as unconstitutional prior restraints—restraining the *presentation* of information.¹⁰ In *44 Liquormart, Inc. v. Rhode Island*, the Court invalidated a statutory prohibition against advertisements that provided the public with accurate information about retail prices of alcoholic beverages—again, a *presentation* of information.¹¹ More recently, the Court in *Kennedy v. Bremerton School District*, concluded that the First Amendment protects religious observance even if the observer is a public employee who desires to pray on public grounds.¹² Yet again, the Court protected a *presentation* of one’s beliefs.¹³

5. NEIL RICHARDS, *INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE* 95 (2017) (“More formally, intellectual privacy is the protection from surveillance or unwanted interference by others when we are engaged in the processes of generating ideas and forming beliefs—when we’re thinking, reading, and speaking with confidants before our ideas are ready for public consumption.”).

6. *Id.* at 96.

7. Wayne Unger, *Stay Out of My Head: Neurodata, Privacy, and the First Amendment*, WASH. & LEE L. REV. (forthcoming 2023); As Neil Richards argued, if intellectual privacy is about *contemplation*, then this is the act of generating new ideas or changing existing ones.

8. *Id.*

9. *See id.* (“First Amendment theory has focused on the *presentation* of ideas, thoughts, and beliefs, like compulsory flag salutes” at issue in *West Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943)).

10. 536 U.S. 150, 153 (2002) (at issue was whether “a village ordinance making it a misdemeanor to engage in door-to-door advocacy without first registering with the mayor and receiving a permit violate[d] the First Amendment.”)

11. 517 U.S. 484, 485 (1996).

12. *Kennedy v. Bremerton School District*, 142 S. Ct. 2407, 2415 (2022) (The Free Exercise and Free Speech Clauses of the First Amendment protect an individual engaging in personal religious observance.”).

13. *See id.*

This prompts the question: if the First Amendment protects individuals' production and presentation of ideas, does it also preclude governmental *access* to or *intrusion* of thoughts and beliefs? I have posited that if ideas, thoughts, and beliefs can be captured and stored as data ("neurodata"),¹⁴ then that data should fall under First Amendment protection given its substance.¹⁵ I have also argued that the First Amendment's protections are more robust than the Fourth Amendment's protection against unreasonable searches and seizures.¹⁶ However, a more comprehensive Fourth Amendment analysis regarding its protection of neurodata has been out of scope for my previous scholarship.¹⁷ I turn to that analysis here.

If Fourth Amendment protections extend to voluminous amounts of intimate personal information like cell phone geolocation logs, as the Supreme Court found in *Carpenter v. United States*, it follows that they should extend to one's internal thoughts as well.¹⁸ Consider Justice Sotomayor's concurrence in *United States v. Jones*, another case regarding geolocation data.¹⁹ In *Jones*, Justice Sotomayor recognized the sensitivity of location data by stating, "GPS monitoring generates a precise comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."²⁰ If GPS data generates a comprehensive record that can illustrate an individual's associations, then certainly neurodata, which arguably is *more* comprehensive and intimate, would also fall under the Fourth Amendment's protections. While it may logically follow that such an extension of Fourth Amendment jurisprudence should occur, a deeper analysis that answers *how* and *why* the Court should extend the Fourth Amendment is required.

14. Neurodata is a broad term that could represent different kinds of data. For instance, brain-testing data from an electroencephalogram (EEG) or magnetic resonance imaging (MRI) could be considered neurodata. However, for this Essay, I use neurodata in the limited context of *substantive* ideas, thoughts, and beliefs captured as storable and processable data.

15. See Unger, *supra* note 7.

16. See *id.* (arguing that the burdens of persuasion for the government and the established presumptions under a First vs. Fourth Amendment challenge illustrate how the First Amendment protections are more robust than the Fourth Amendment protections).

17. *Id.* ("To be clear, whether the Fourth Amendment protects against government intrusion of neurodata, and the extent to which that protection exists, is not considered here.")

18. *Carpenter v. United States*, 138 S. Ct. 2206, 2216–20 (concluding that modern technologies have great consequences for privacy because such technology has the capability to capture every detail of an individual's life); At issue in *Carpenter* was whether a warrantless search of a defendant's cell site location information from his cell phone service provider violates the Fourth Amendment's protection against unreasonable searches and seizures. The Court concluded that it did; see Wayne Unger, *Katz and Covid-19: How a Pandemic Changed the Reasonable Expectation of Privacy*, 12 HASTINGS SCI. & TECH. L.J. 40, 58 (2020) [hereinafter "Katz & COVID"].

19. 565 U.S. 400 (2012).

20. *Id.* at 415 (Sotomayor, J., concurring).

This Essay will present the next era of privacy protections to confront an emerging frontier of privacy risks: the battle for your brain, as Professor Nita Farahany describes it.²¹ If we can capture ideas, thoughts, and beliefs as storable and processable data, what constitutional protections should extend to protect that data, if any? This Essay argues that current Fourth Amendment jurisprudence should—and must—extend to neurodata. I begin by reviewing the emerging technology that, with further research and development, will likely capture and store neurodata. Next, I analyze whether neurodata falls within the Fourth Amendment zone of protection. Then, I demonstrate how existing Fourth Amendment jurisprudence extends to neurodata and protects ideas, thoughts, and beliefs as data. Last, I provide a normative evaluation to justify this extension.

I. Neurodata-Capturing Technologies & Fourth Amendment Searches of the Brain

Once science-fiction, the idea of mind-reading is now within reach of being a reality. While it requires more research and development, recent advancements in brain-computer interfaces (“BCI”) and artificial intelligence (“AI”) have enabled, albeit in its infancy, the real-time collection and decoding of brain signals.²² In 2021, researchers at the University of California, San Francisco (“UCSF”) successfully “decoded sentences from [the study’s] participant’s cortical activity in real time”²³ But UCSF is not alone. Neuro-startups, such as Synchron and Elon Musk’s Neuralink, are developing medical implants to do the same.²⁴ Synchron, for example,

21. NITA FARAHANY, *THE BATTLE FOR YOUR BRAIN: DEFENDING THE RIGHT TO THINK FREELY IN THE AGE OF NEUROTECHNOLOGY* (2023).

22. See David A. Moses, Ph.D. et al., *Neuroprosthesis for Decoding Speech in a Paralyzed Person with Anarthria*, 385 N. ENG. J. MED. 217 (2021) [hereinafter the “UCSF Study”]; Anika Binnendijk et al., *Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment*, RAND CORP. 3 (2020), https://www.rand.org/pubs/research_reports/RR2996.html (discussing advancements in BCIs and its future implications for the U.S. Military to expand and improve human-machine teaming); P.R. Roelfsema et al., *Mind Reading and Writing: The Future of Neurotechnology*, 22 TRENDS IN COGNITIVE SCI. 598 (2018) (providing an overview of methods to interface with the brain, speculating about potential applications, and discussing important issues associated with a neuro-technologically assisted future); Shinji Nishimoto et al., *Reconstructing Visual Experiences from Brain Activity Evoked by Natural Movies*, 21 CURRENT BIOLOGY 1641 (2011) (the results of this study “demonstrate[d] that dynamic brain activity measured under naturalistic conditions can be decoded using current fMRI technology.”); but see Emily Murphy & Jesse Rissman, *Evidence of Memory from Brain Data*, J.L. & THE BIOSCI. 1, 5–6 (2020) (“Presently, no brain-based memory detection technology functions as one might imagine ‘mind-reading’ to work, via un-cued reconstruction of the subjective contents of a subject’s memory.”).

23. UCSF Study, *supra* note 22.

24. Alena Botros, *Elon Musk’s Neuralink Brain Computer Startup Is Beat Again. This Time a Competitor Implanted its Device into its First U.S. Patient*, FORTUNE MAG. (July 18, 2022), <https://fortune.com/2022/07/18/elon-musk-neuralink-beat-by-synchron-brain-computer-startup->

implanted its Stentrode device, which connects a computing device implanted in the patient's chest to an external computing device via Bluetooth, into a blood vessel of a patient's motor cortex.²⁵ The Stentrode then translates the signals in real-time using artificial intelligence ("AI").²⁶

Artificial intelligence generally refers to the "science and engineering of making intelligent machines, especially intelligent computer programs," according to IBM.²⁷ AI combines computer science and robust datasets to enable problem-solving.²⁸ In practice, AI's problem-solving capabilities output predictions, such as what a brain signal indicates.²⁹

Brain-computer interfaces are not new. Rather, the AI-enablement is new as it has created new capabilities for BCIs. For instance, older BCI technologies include spelling systems that display a series of letters.³⁰ When a person with amyotrophic lateral sclerosis ("ALS") sees the letter that they want, the BCI reads a blip in their brainwave and interprets it as a "key-stroke."³¹ In this example, a person with ALS is interacting with a BCI, but the BCI is not "reading the person's mind," so to speak, because it is not actively decoding or interpreting the signal into substantive information.³²

Take Dr. Scott Mackler as another example. Dr. Mackler was a renowned addiction researcher at the University of Pennsylvania prior to his death in 2013.³³ For years after he was diagnosed with ALS in April 1999, he "communicated by shifting his eyes slightly to the left or right, indicating

us-human-trial/ (comparing Synchron to Neuralink—another startup that is focused on BCIs and the technology to implant them).

25. Ashlee Vance, *Brain-Computer Interface Startup Implants First Device in US Patient*, BLOOMBERG BUSINESSWEEK (July 18, 2022), <https://www.bloomberg.com/news/articles/2022-07-18/brain-computer-interface-company-implants-new-type-of-device> (Synchron was founded in 2016 and funded by Khosla Ventures, Max Hodak, and Thomas Reardon—the latter two of whom are well-known BCI experts. Its Stentrode can be inserted into the brain without cutting through a person's skull. To implant the Stentrode, a doctor makes an incision in the patient's neck and feeds the Stentrode through the jugular vein and into a blood vessel in the motor cortex. A subsequent procedure connects the Stentrode to a computing device implanted into the patient's chest. The Stentrode reads the brain signals when neurons fire, the computing device amplifies the signals, and via Bluetooth, another computing device translates the signals.)

26. *Id.*

27. *What is Artificial Intelligence?*, IBM, <https://www.ibm.com/topics/artificial-intelligence>.

28. *Id.*

29. *Id.*

30. Betts Peters, *FYI: Brain-Computer Interfaces (BCI)*, ALS ASS'N (June 10, 2020), <https://www.als.org/navigating-als/resources/fyi-brain-computer-interface-bci>.

31. *Id.*

32. See OWEN JONES ET AL., *LAW & NEUROSCIENCE* 825 (2d ed. 2021) (describing BCI systems that detect brain signals and convert, not decode or interpret, into commands to move a computer cursor) [hereinafter "LAW & NEUROSCIENCE"].

33. *The Scott A. Mackler, MD, PhD, Assistive Technology Program*, ALS ASS'N, <https://www.als.org/florida/local-care-services/scott-mackler-assistive-technology-program>.

letter-by-letter what he was trying to spell out.”³⁴ Advancements in neuroscience and BCI technology eventually led to an EEG-powered device that “picked up signals from [Dr. Mackler’s] neurons, or brain cells.”³⁵ The signals were then translated into alphabetic letters that allowed Dr. Mackler to communicate.³⁶

Dr. Mackler’s case exemplifies the development of BCI technology. More specifically, it shows how BCI advancements have led to an increase in the human interaction component. As professors and neuroscientists Owen Jones, Jeffrey Schall, and Francis Shen assert, “[d]ecoding the meaning of neural impulses is a very active area of current research.”³⁷ As these decoding capabilities advance, they can and will produce neurodata.³⁸

This Essay presumes that BCIs will advance to such an extent as to produce neurodata—substantive ideas, thoughts, and beliefs as storable and processable data. It further presumes a proliferation of BCIs will occur over the next decade or two. With these presumptions in mind, I return to the constitutional question of this Essay—whether the Fourth Amendment will apply to searches of neurodata. In the next section, I turn to the start of a Fourth Amendment analysis.

II. Unreasonable Searches of Intimate Data

The Fourth Amendment protects individuals from unreasonable searches and seizures.³⁹ Its purpose is to “safeguard the privacy and security of individuals” against arbitrary invasions by government officials.⁴⁰ When James Madison drafted the Fourth Amendment, he captured the general sentiment of the colonial era, which was clear opposition to the general warrants and writs of assistance that allowed the British to invade and search persons’

34. *Id.*; Seth Zweifler, *Scott Mackler, Pioneering Penn Professor, Dies*, THE DAILY PENNSYLVANIAN (Nov. 14, 2013), <https://www.thedp.com/article/2013/11/scott-mackler-obituary>.

35. Denise Schrier Cetta, *The Passing of Pioneering Brain Scientist*, CBS NEWS (Nov. 17, 2013), <https://www.cbsnews.com/news/the-passing-of-pioneering-brain-scientist/>; *see generally* LAW & NEUROSCIENCE at 107 (EEG stands for electroencephalograph, which is a recording method that detects weak electrical signals from the surface of the head).

36. Cetta, *supra* note 3635; LAW & NEUROSCIENCE at 824.

37. LAW & NEUROSCIENCE at 827. Owen Jones is the Glenn M. Weaver, M.D. and Mary Ellen Weaver Chair in Law, Brain, and Behavior and Professor of Law and Biological Sciences at Vanderbilt University; Jeffrey Schall is the E. Bronson Ingram Professor of Neuroscience at Vanderbilt University; Francis Shen is Professor of Law at University of Minnesota Law School and Instructor in Psychology at Harvard Medical School.

38. *See supra* note 14; this Essay uses the term “neurodata” to mean substantive ideas, thoughts, and beliefs captured as storable and processable data.

39. U.S. CONST. amend. IV; The Fourth Amendment provides, in relevant part, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause”

40. *Carpenter v. United States*, 138 S. Ct. 2206, 2231 (2018).

homes.⁴¹ While the Amendment's roots are planted in protecting individuals' homes from arbitrary trespasses by government officials, the Supreme Court has extended the Fourth Amendment's protections to personal information.⁴²

A. The Reasonable Expectation of Privacy Test

Through Justice Harlan's concurring opinion, *Katz v. United States* introduced the "reasonable expectation of privacy" test for the Fourth Amendment.⁴³ In that case, law enforcement recorded the defendant, Charles Katz, transmitting wagering information by telephone in a public telephone booth.⁴⁴ The Supreme Court reversed Katz's conviction because the recording violated his Fourth Amendment protection from unreasonable searches.⁴⁵

The *Katz* "reasonable expectation of privacy" test has served as the foundational inquiry in more recent informational privacy cases. In *Carpenter v. United States*, the Supreme Court concluded that "when the Government tracks the location of a cell phone, it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."⁴⁶ The Court in *Riley v. California* also acknowledged that "modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."⁴⁷ But perhaps Justice Sotomayor, in *United States v. Jones*, best underscored the sensitivity of personal data.⁴⁸ In her *Jones* concurrence, she stated that a person's cell phone data can provide a comprehensive record of one's associations.⁴⁹ The Court in *Carpenter*, *Riley*, and *Jones* found a reasonable expectation of privacy with respect to voluminous personal information. In each of these cases, the defendant had a reasonable expectation that his data would be kept private, even when that data is shared with or is accessible by a third-party.

41. *Riley v. California*, 573 U.S. 373, 403 (2014).

42. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2218 (providing "when the Government tracks the location of a cell phone it achieves near perfect surveillance" and finding that such capability leads to a reasonable expectation of privacy for the individual).

43. 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see generally* Katz & COVID, *supra* note 18, at Part II.B (further explaining Justice Harlan's reasonable expectation of privacy test).

44. *Katz*, 389 U.S. at 348.

45. *Id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents ignored 'the procedure of antecedent justification . . . that is central to the Fourth Amendment,' a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case.").

46. *Carpenter*, 138 S. Ct. at 2218.

47. *Riley*, 573 U.S. at 393.

48. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

49. *See id.*

Taken together, these cases, along with others not mentioned herein, illustrate the well-established analysis framework for Fourth Amendment questions. First, does the challenged act(s) by the Government constitute a search or seizure?⁵⁰ Second, if so, was the search or seizure reasonable?⁵¹ Assuming a search has occurred, courts apply either a physical trespass test or the reasonable expectation of privacy test from *Katz*.⁵² For the latter, if an individual holds a reasonable expectation of privacy, then the search is subject to the warrant requirement, unless a specific exception applies.⁵³ If an individual does not hold a reasonable expectation of privacy, then a warrant is not necessary.⁵⁴

B. Is it a search?

Proceeding in that order, does a search of neurodata fall within the Fourth Amendment's zone of protection? Certainly, the answer is yes. But does *mere access* of one's neurodata by a government official constitute a search? Surely, the answer must be yes as well.

Carpenter and *Riley* are instructive here. While law enforcement analyzed *Carpenter*'s cell site location information ("CSLI"), the Court concluded that the *mere acquisition* of the CSLI constituted a search within the meaning of the Fourth Amendment.⁵⁵ And in *Riley*, a law enforcement officer conducted an improper search incident to *Riley*'s arrest when the officer *accessed* the information on *Riley*'s cell phone.⁵⁶ Accordingly, if *mere access* was sufficient to constitute a search in *Riley*, then certainly, *mere access* of an individual's neurodata constitutes a search as well. *Carpenter* and *Jones* lend support to this inference as well.

If *mere acquisition* of personal information is sufficient to constitute a search in *Carpenter*, then *access* must be sufficient even if a government

50. *Kyllo v. United States*, 533 U.S. 27, 31 (2001) ("the antecedent question whether or not a Fourth Amendment 'search' has occurred is not so simple under our precedent.").

51. *Id.*

52. At common law, the trespassory test asks whether there was a physical intrusion or entry without authorization by law; see *Jones*, 565 U.S. at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.") (emphasis in the original); *Katz*, 389 U.S. at 512 (concluding that the recording of an individual in a public telephone booth constituted a search within the meaning of the Fourth Amendment before assessing the reasonableness of the search).

53. *Id.* at 514.

54. See *id.*

55. *Carpenter*, 138 S. Ct. at 2221 ("Having found that the acquisition of *Carpenter*'s CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.").

56. *Riley*, 573 U.S. at 378 (at issue in *Riley* was not whether the officer's actions constituted a search, but rather whether the search incident to arrest exception applied to the search of *Riley*'s phone).

official does not take possession or custody of one's neurodata. Acquisition simply means the act of coming into possession or control.⁵⁷ By this definition, an individual may *acquire* personal information, but not access, review, read, or analyze it. For example, Person A may acquire the file that contains Person B's CSLI, like in *Carpenter*, but need not open the file and read it for the *mere acquisition* to constitute a Fourth Amendment search. Accordingly, it follows, that even if a government official does not *acquire* the file of personal information, *accessing* the file is more offensive to the Fourth Amendment because the government official can read, analyze, and review the data contained therein.

Thus, *mere access* of an individual's neurodata by a government official constitutes a search, at least under the Court's *Riley* and *Carpenter* precedents. However, *mere access* of any ordinary data does not necessarily mean that the Fourth Amendment protections should attach. To expand on this point, I turn to the third-party doctrine.

The third-party doctrine "traces its roots to [*United States v.*] *Miller*" and *Smith v. Maryland*.⁵⁸ Read together, those cases provided that an individual does not hold a reasonable expectation of privacy under the *Katz* test in the information he "voluntarily convey[s]" to a third-party.⁵⁹ In *Miller*, the information at issue was bank records held by the defendant's banks.⁶⁰ In *Smith*, it was the Government's capture of outgoing phone numbers dialed through the use of a pen register.⁶¹

But not all data and information is alike. The *Carpenter* Court distinguished CSLI from the information at issue in both *Miller* and *Smith*.⁶² Unlike bank records and a log of phone numbers dialed, which are limited in their substance and do not contain any confidential communications, CSLI is highly revealing as it provides "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."⁶³

57. *Acquisition* and *Acquire*, MERRIAM-WEBSTER.COM, <https://www.merriam-webster.com/dictionary/acquire> (last visited Feb. 15, 2023).

58. *See generally* *United States v. Miller*, 425 U.S. 435 (1976); *see also* *Smith v. Maryland*, 442 U.S. 735 (1979).

59. *Smith*, 442 U.S. at 744; Courts may apply the reasonable expectation of privacy test from *Katz* to determine the search's reasonableness.

60. *Carpenter*, 138 S. Ct. at 2216 (summarizing *Miller*, "While investigating *Miller* for tax evasion, the Government subpoenaed his banks [for] canceled checks, deposit slips, and monthly statements.")

61. *Id.* (summarizing *Smith*, "The Court ruled that the Government's use of a pen register—a device that recorded the outgoing phone numbers dialed . . . was not a search [because] subscribers know, after all, that the numbers are used by the telephone company for a variety of legitimate business purposes . . .") (internal quotation marks omitted).

62. *See generally* *Carpenter*, 138 U.S. at 2219–20 (describing the data at issue in both cases).

63. *Id.* ("*Miller* likewise noted that checks were 'not confidential communications but negotiable instruments' . . . There is a world of difference between the limited types of personal

Fundamentally, the data at issue in these cases differ not only on their substance, but also on how the data was generated or collected.

There are three types of digital personal information that stem from third-party data collection. First, user-provided data is information that the user provides to the third-party.⁶⁴ Second, queried data is information that the third-party sources or procures about the user.⁶⁵ Third, autogenerated data is information that is automatically created and collected, such as CSLI.⁶⁶ In comparing the three types, each type almost always carries a different expectation of privacy. For instance, if a user voluntarily conveys information about herself to a third-party, then most clearly, the user does not hold any reasonable expectation of privacy just as the third-party doctrine provides.⁶⁷ However, if a third-party automatically generates and collects data about a user, then the user probably has a reasonable expectation of privacy—even if the user is unaware of the data generation and collection—like CSLI in *Carpenter*.⁶⁸

While the Court has not set forth an exacting test to determine whether a search has occurred, Professor Matthew Tokson has surveyed the Court's Fourth Amendment jurisprudence and deduced three general principles that the Court seemingly follows when determining whether an asserted privacy expectation is reasonable.⁶⁹ They are: the intimacy, the amount, and the cost of collection.⁷⁰ In short, the more intimate and voluminous the data

information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by [cell phone services providers] today.”).

64. Wayne Unger, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion*, 22 COLUM. SCI. & TECH. L. REV. 308, 329 (2021).

65. *Id.*

66. *Id.* (CSLI is automatically captured and stored by the cell phone service provider).

67. *Id.*

68. *Id.* at 329–31; see Reply Brief for Petitioner at 9–10, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 4838412 (U.S.), at *9–10 (U.S., Oct. 24, 2017) (“And while some users may be vaguely aware that their phones have to connect to cell towers, few if any are likely to know that every such connection is recorded and maintained, even when one turns off location services on one’s phone.”); Brief of the Ctr. for Democracy & Tech. as Amicus Curiae in Support of Petitioner at 3–4, 2017 WL 3530958 (U.S.), at *3–4 (U.S., Aug. 14, 2017) (“The changes resulting from digital technology . . . and third parties creating databases of personal information not previously available – make it eminently reasonable to conclude that Americans have a legitimate expectation of privacy with respect to much of this information.”); cf. *United States v. Bledsoe*, No. CR 21-204 (BAH), 2022 WL 3594628, at *8 (D.D.C. Aug. 22, 2022) (in distinguishing user-generated location information from CSLI, the district court concluded, “unlike CSLI . . . the only way that Facebook was able to determine when and where a user engaged in account activity on January 6, 2021, is by virtue of the user making an affirmative and voluntary choice to download the Facebook or Instagram application . . . create an account . . . and, critically, take no available steps to avoid disclosing his location . . .”).

69. See Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1 (2020) [hereinafter “Tokson’s Principles”].

70. *Id.* at 14.

is, the more likely that the data is subject to the Fourth Amendment's protections (including its warrant requirement) because the reasonableness of any privacy expectations increases.⁷¹ This aligns with the Court's jurisprudence. *Carpenter's* CSLI is more intimate than *Miller's* bank records, for example, and it is more voluminous than *Smith's* log of telephone numbers dialed.

Furthermore, Tokson's principles also align with the three data types described above. Autogenerated data is almost certainly more voluminous because it can be captured automatically at a low cost (e.g., CSLI). User-provided data is not voluminous in nature because the user must affirmatively provide it, and presumably, the user is less likely to provide highly intimate data about himself. Accordingly, given the nature of autogenerated data, it is more likely to fall under the Fourth Amendment's protections than user-provided data.

Let us return to neurodata and consider it to be a form of user-provided data, specifically. If a data subject or user expressly or implicitly consents to a third-party's collection of their neurodata using a BCI, then the third-party doctrine *may* be triggered. A textualist interpretation of the third-party doctrine provides that, if user-provided data is *voluntarily conveyed* to a third-party, then the data subject does not have a reasonable expectation of privacy with respect to that data.⁷² The question becomes whether the user's express or implicit consent to the collection of her neurodata constitutes "voluntary conveyance." If the question is limited to that, and only that, then *Miller* is instructive. It is reasonable to conclude that *Miller* consented to the bank's keeping records when he decided to use the bank's services. This is no different than a user consenting to a BCI-provider—when an individual uses the provider's services, he expressly or implicitly volunteers his neurodata.⁷³

However, if the inquiry is expanded beyond the voluntary conveyance determination, then *Carpenter* is instructive because there is a "qualitative difference" with respect to neurodata.⁷⁴ As the Court demonstrated in

71. *Id.* at 15–18.

72. *Smith*, 442 U.S. at 743 (a person "has no legitimate expectation of privacy in information he *voluntarily turns over* to third parties.") (emphasis added); see Bledsoe, 2022 WL 3594628 at *7 ("[T]he sharing [of information] in prior third-party cases rested on 'voluntary exposure' that the *Carpenter* Court found to be absent in the context of CSLI records."); Wayne Unger, *You're Likely Protected: Smart Cities, Big Data, and Fourth Amendment Privacy Protections*, ABA'S THE SCITECH LAWYER (Winter 2022), <https://tinyurl.com/jf2v9uc8> (analyzing the text of the third-party doctrine).

73. This assumes the BCI-provider stores the data subject's neurodata after it is collected.

74. See *Carpenter*, 138 S. Ct. at 2216 ("But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of [CSLI].").

Carpenter, an analysis of the data's nature is necessary in determining whether a search has occurred. Neurodata, by its aforementioned presumptive definition, is *highly* intimate—so intimate, in fact, that it could be considered the most personal type of data that exists with respect to its substance.⁷⁵

We can restate the foregoing as this: a user who takes affirmative action that either expressly or implicitly provides the data subject's consent for a third-party to collect and store neurodata is, standing alone, insufficient to determine whether the third-party doctrine should apply. As the Court has made clear, whether a dataset is subject to the warrant requirement depends on the nature of the data itself. In Professor Matthew Tokson's framework, that requires an analysis of the dataset's intimacy, amount, and cost.⁷⁶

The same is true if the neurodata is autogenerated. Autogenerated neurodata would fall within the Fourth Amendment's zone of protection because, as previously stated, it would almost certainly be more voluminous than user-provided neurodata. But even if it were not more voluminous than a user-provided neurodata-set, the intimacy considerations are nonetheless sufficient to place autogenerated neurodata within the Fourth Amendment's zone of protection.

Thus, regardless of the route taken in the analysis, neurodata is protected by the Fourth Amendment. The pathway may be the mere *acquisition* of neurodata. Another pathway may be mere *access* to the neurodata. Beyond these, another pathway may be via an intimacy analysis. All of these pathways lead to the same determination that neurodata is protected by the Fourth Amendment.

C. Was It Reasonable?

The next threshold question is whether the search is reasonable. Ultimately, the measure as to whether a government search is constitutional is its reasonableness.⁷⁷ Absent consent or a lawful warrant, determining reasonableness is not an exact science.⁷⁸ With respect to informational privacy, the Court has provided some guidance in the more recent cases mentioned above. In *Riley*, the Court declared, “[i]n the absence of a warrant, a search is reasonable *only if* it falls within a specific exception to the warrant

75. See Neurodata, *supra* note 14 (providing the definition for neurodata).

76. Tokson's Principles, *supra* note 69, at 14.

77. *Carpenter*, 138 S. Ct. at 2221; see Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 801 (1994) (the Fourth Amendment simply “require[s] that all searches and seizures be reasonable.”).

78. See *e.g.*, *Terry v. Ohio*, 392 U.S. 1, 20–21 (1968) (“there is no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails.”) (internal quotation marks omitted).

requirement.”⁷⁹ Put another way, it is well-established that a warrantless search or seizure of someone, something, or someplace that falls within the protection of the Fourth Amendment is presumptively unreasonable.⁸⁰

For bodily autonomy, perhaps another set of cases from the federal judiciary is instructive here given the nature of neurodata. In *Winston v. Lee*, the Supreme Court heard a petition for a permanent injunction where Virginia sought to compel a suspect, accused of armed robbery, to undergo a surgical procedure to remove a bullet lodged in his chest for evidentiary purposes.⁸¹ According to the Court, a surgical procedure, especially one under a general anesthetic, implicates the most “personal and deep[ly]-rooted expectations of privacy.”⁸² A compulsory intrusion *into* an individual’s body offends the Fourth Amendment in the highest magnitude, such that the intrusion may be unreasonable even if it is likely to produce evidence of a crime.⁸³ In balancing the suspect’s dignitary interests in personal privacy and bodily integrity against Virginia’s proffered “compelling interest” in obtaining evidence of a crime, the Court granted the injunction and held that the “operation sought [would] intrude substantially on respondent’s protected interests.”⁸⁴ The *Winston* Court effectively applied a compelling interest standard (i.e., strict scrutiny) that also considered whether a sought-after intrusion is “not more intrusive than reasonably necessary to accomplish its goals.”⁸⁵

Searches that intrude upon a person’s dignitary interests in personal privacy and bodily integrity are even *more* offensive and unreasonable when they are exploratory in nature. Take *Sanchez v. Pereira-Castillo*, for example. In that case, officers subjected a prisoner to numerous bodily invasive searches, including strip-searches, x-rays, forced bowel movements, rectal examinations, and lab tests.⁸⁶ Even though these searches failed to reveal the presence of contraband—the object of the officers’ searches—they proceeded to have a surgeon conduct an exploratory surgery of the prisoner’s

79. *Riley*, 573 U.S. at 382.

80. *Mincey v. Arizona*, 437 U.S. 385, 390 (1978) (“[I]t is a cardinal principle that ‘searches conducted outside the judicial process, without prior approval by a judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.’”) (quoting *Katz*, 389 U.S. at 357); *Kentucky v. King*, 563 U.S. 452, 459 (2011) (“It is a basic principle of Fourth Amendment law, we have often said, that searches and seizures inside a home without a warrant are presumptively unreasonable.”) (internal quotation marks omitted).

81. 470 U.S. 753, 755 (1985).

82. *Id.* at 760 (citing *Schmerber v. California*, 384 U.S. 757, 768 (1966)).

83. *Id.* at 759.

84. *Id.* at 767.

85. *Id.* at 759.

86. 590 F.3d 31, 37 (1st Cir. 2009).

abdomen under total anesthesia.⁸⁷ In determining the reasonableness of the search, the *Sanchez* Court assessed “the scope of the particular intrusion, the manner in which it [was] conducted, the justification for initiating it, and the place in which it [was] conducted.”⁸⁸ Ultimately, the First Circuit Court of Appeals concluded that the compulsory exploratory surgery was highly violative to the prisoner’s Fourth Amendment protections regardless of the state’s proffered purpose in ensuring the proper and safe administration of a correctional facility.⁸⁹

Regardless of whether bodily integrity or informational privacy is at issue, the presumption that warrantless searches are unreasonable can be rebutted by asserting an exception to the warrant requirement.⁹⁰ At issue in *Riley* was the applicability of one of those exceptions: a search incident to an arrest.⁹¹ *Carpenter* described another exception: exigent circumstances. Exigencies that may excuse the warrant requirement, assessed on a case-by-case basis, include “the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence.”⁹² But none of these exceptions apply to a neurodata search given the sensitivity and intimacy of the “thing” searched.

While the *Carpenter* Court recognized that there could be “fact-specific threats” that would justify the warrantless collection of CSLI,⁹³ the

87. *Id.* at 38 (the First Circuit Court of Appeals found the surgeon to be a state actor, even though the surgeon was employed by a private hospital, because her actions were “under the color of law” and “strongly encouraged by the correctional [officers]” under the state compulsion test. The state compulsion test asks whether the state has exercised coercive power or has provided such significant encouragement, either overt or covert, over a private party such that the challenged conduct must be deemed to be that of the state.)

88. *Id.* at 43 (citing *Bell v. Wolfish*, 441 U.S. 520, 559 (1979)).

89. *Id.* at 48.

90. There is significant debate regarding the meaning of the Fourth Amendment, the validity of the warrant requirement, and the applicability of the warrant requirement; *e.g.*, *California v. Acevedo*, 500 U.S. 565, 581 (1991) (Scalia, J., concurring) (“The Fourth Amendment does not by its terms require a prior warrant for searches and seizures; it merely prohibits searches and seizures that are ‘unreasonable’ . . . What [the Fourth Amendment] explicitly states regarding warrants is by the way of limitation upon their issuance rather than a requirement of their use.”); *see also* Craig Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473–1474 (1985) (providing a then-current list of the exceptions to the Fourth Amendment warrant requirement).

91. *Id.* at 383 (explaining the case law that gave rise to the search incident to an arrest doctrine).

92. This Essay excludes analyses regarding these other exceptions because they are either less relevant or irrelevant to the Fourth Amendment question regarding neurodata; *see* *Carpenter*, 138 S. Ct. at 2223 (recognizing other exceptions to the Fourth Amendment’s warrant requirement, such as international border searches, the automobile exception, inventory searches, etc.).

93. *See* *Missouri v. McNeely*, 569 U.S. 141, 151 (2013) (“The State properly recognizes that the reasonableness of a search under the exigency exception to the warrant requirement must be evaluated based on the totality of the circumstances.”); *Carpenter*, 138 S. Ct. at 2223 (recognizing that “fact-specific threats will likely justify the warrantless collection of CSLI [such as] bomb

Court has also recognized that courts should balance governmental intrusion against the sensitivity and intimacy of the “thing” searched, especially under the “exigent circumstances” doctrine.⁹⁴ Take, for example, the bodily autonomy applications provided above and in another case: *Birchfield v. North Dakota*. In *Birchfield*, the Court concluded that breath tests are significantly less intrusive than blood tests, and because of this, a breath test, but not a blood test, may be administered as a warrantless search incident to a lawful arrest.⁹⁵ The Court determined that the physical intrusion of a breath test is “almost negligible” because they “do not require piercing the skin,” but rather, only a “minimum of inconvenience.”⁹⁶ Further, the Court established that blood tests “are a different matter” because they require piercing of the skin and “extract a part of the subject’s body.”⁹⁷

Both the *Sanchez* and *Winston* Courts essentially applied the same balancing test as *Birchfield*—balancing the government intrusion against the sensitivity and intimacy of the search. But, of course, unlike a blood test, *Sanchez* and *Winston* presented significantly more intrusive bodily searches that, to a certain extent, “shock[ed] the conscience” of the courts.⁹⁸ It is also important to note that a bodily search need not *physically* invade an individual’s body to be violative of the Fourth Amendment.⁹⁹ Courts have also found that physical invasiveness and risk of physical or emotional harm are relevant, but not dispositive, in determining whether a bodily search is

threats, active shootings, and child abductions. Our decision today does not call into doubt warrantless access to CSLI in such circumstances.”).

94. *E.g.*, *Birchfield v. North Dakota*, 579 U.S. 438, 461 (2016) (“[In this case], we engage in the same mode of analysis as in *Riley*: [w]e examine the degree to which they intrude upon an individual’s privacy and . . . the degree to which they are needed for the promotion of legitimate governmental interests.”) (some brackets in the original omitted); *Carpenter*, 138 S. Ct. 2206 (holding that the nature of CSLI is fundamentally different, and accordingly, should be afforded a heightened level of protection by not extending the third-party doctrine); *Birchfield*, 579 U.S. at 474–76 (finding that blood tests are significantly more intrusive, and thus more deserving for greater Fourth Amendment protections, than breath tests).

95. *Birchfield*, 579 U.S. at 476; *cf. Mitchell v. Wisconsin*, 139 S. Ct. 2525, 2531 (2019) (holding that in circumstances where a suspected intoxicated driver is unconscious, “the exigent-circumstances rule almost always permits a blood test without a warrant [because] [w]hen a breath test is impossible, enforcement of the drunk-driving laws depends on the administration of a blood test.”).

96. *Birchfield*, 579 U.S. at 461.

97. *Id.* at 465; *McNeely*, 569 U.S. at 148 (blood draws are “a compelled physical intrusion beneath [the defendant’s] skin and into his veins.”).

98. While the *Sanchez* Court did not use the term “shock the conscience” in its ruling, a fair and reasonable reading of the opinion shows that the *Sanchez* Court was shocked at the allegations asserted by the plaintiff; *see, e.g.*, *Sanchez*, 590 F.3d at 44 (“The most disturbing element of the exploratory surgery is unquestionably its scope.”) (internal quotation marks omitted); *see United States v. Booker*, 728 U.S. 535, 537 (6th Cir. 2013) (using the term “shock the conscience.”).

99. *See Sims v. Labowitz*, 885 F.3d 254 (4th Cir. 2018) (concluding that photographing a minor’s erect penis for evidentiary purposes violates the Fourth Amendment).

unconstitutionally intrusive.¹⁰⁰ Seemingly, the government must meet an exceptionally high bar to justify an intrusive search into one's body—like the compelling interest standard provided in *Winston*.

Privacy interests do not disappear altogether, even with a valid warrant. In *Sims v. Labowitz*, the Fourth Circuit recognized that a valid warrant did not immunize law enforcement from a §1983 complaint stemming from a Fourth Amendment search.¹⁰¹ In that case, a detective obtained a search warrant that authorized a detective to photograph a suspect's naked body, including his erect penis.¹⁰² The suspect, however, was a minor.¹⁰³ During the execution of the warrant, the detective allegedly demanded that the minor “manipulate his penis to achieve an erection.”¹⁰⁴ While, unlike *Sanchez* and *Winston*, there was no penetration of the skin or surgical operation,¹⁰⁵ the Fourth Circuit Court of Appeals nonetheless concluded, “a reasonable police officer would have known that attempting to obtain a photograph of a minor child's erect penis, by ordering the child to masturbate in the presence of others, would unlawfully invade the child's right to privacy under the Fourth Amendment.”¹⁰⁶ In this regard, the minor's privacy interests superseded a valid search warrant. Here, the sensitivity and intimacy of the search unquestionably outweighed the state's interest in obtaining evidence of the crime alleged against the minor.¹⁰⁷

While judicial scrutiny may differ, physical location is no different with respect to privacy interests, albeit less sensitive than intrusive bodily searches. It is widely recognized and accepted that the Fourth Amendment protects a “variety of settings,” but none is more clear than “when bounded by the unambiguous physical dimensions of an individual's home”¹⁰⁸ This general principle stems from, “the right of a man to retreat into his own

100. *Id.* at 261.

101. *Id.* at 258.

102. *Id.* at 258–59 (it is important to note that the search warrant was not challenged before it was executed. Sims' attorney was notified of the search warrant *after* law enforcement attempted to photograph Sims. Presumably, Sims' attorney never had to file a motion to suppress the evidence because Sims was unable to achieve an erection during the warrant's execution, and the case settled several months after the Fourth Circuit Court of Appeals issued its decision); *see* Min. Entry, *Sims v. Richardson et al.*, 1:16CV00572 (May 17, 2018).

103. *Sims*, 885 F.3d at 257.

104. *Id.* at 258.

105. *See id.* at 260 (defendants argued that there was no Fourth Amendment violation because the search “did not place Sims at risk of physical harm, and because the search did not physically invade Sims' body.”).

106. *Id.* at 258.

107. *See id.* at 257 (accusing Sims of sending sexually explicit photographs and videos of himself to his 15-year-old girlfriend).

108. *Payton v. New York*, 445 U.S. 573, 589 (1980).

home and there be free from unreasonable governmental intrusion.”¹⁰⁹ Or, as the Court has also recognized, “[f]reedom in one’s own dwelling is the archetype of the privacy protection secured by the Fourth Amendment; conversely, physical entry of the home is the chief evil against which [it] is directed.”¹¹⁰ While the exigent circumstances doctrine can apply to the home, its validity and applicability to any particular circumstance or setting nonetheless depends on the level of intrusiveness, the fact-specific threats, and proportionality.¹¹¹

Data is also no different, as the *Carpenter* Court held, and for the aforementioned reasons which I need not repeat here.¹¹²

Returning to neurodata, none of these exceptions, regardless of the totality of the circumstances presented, justify a warrantless search of one’s neurodata. Certainly, a search of a suspect’s neurodata would be the *most intrusive* with respect to the suspect’s bodily autonomy, in both the physical and non-physical senses. If a blood test generally requires a warrant, except in a narrow set of circumstances like an unconscious suspect,¹¹³ then it follows that a neurodata search must also require a warrant given neurodata’s hyper-revealing nature compared to blood samples.¹¹⁴ But even then, the government’s interest in obtaining evidence of a crime, for example, is insufficient in justifying a physical intrusion into one’s body (e.g., the exploratory abdominal surgery in *Sanchez*) as courts can point to other discoverable evidence that does not involve bodily intrusion.¹¹⁵

As the *Sims* Court recognized, even with a warrant, privacy interests do not vanish altogether.¹¹⁶ A search, even with a warrant, need not physically intrude beneath the individual’s skin for their privacy interests to be

109. *Silverman v. United States*, 365 U.S. 505, 511 (1961); *see also Florida v. Jardines*, 569 U.S. 1, 6–7 (2013); *Collins v. Virginia*, 138 S. Ct. 1663, 1670 (2018) (quoting *Silverman*, 365 U.S. at 511, and *Jardines*, 569 U.S. at 6).

110. *Lange v. California*, 141 S. Ct. 2011, 2018 (2021) (internal quotation marks omitted) (quoting *Payton*, 445 U.S. at 585, 587).

111. *E.g.*, *United States v. Cooks*, 920 F.3d 735, 746 (11th Cir. 2019) (validating the exigency asserted by law enforcement—that they had probable cause to believe the suspect’s crawlspace underneath the home contained hostages—and finding that the “search” of the crawlspace was proportional to the risk to human life).

112. *See* discussion *infra* Part II.B.

113. *Mitchell*, 139 S. Ct. at 2531.

114. *Birchfield*, 579 U.S. at 464 (“[A] blood test, unlike a breath test, places in the hands of law enforcement authorities a sample that can be preserved and from which it is possible to extract information beyond a simple BAC reading.”); *Carpenter*, 138 S. Ct. at 2219–20 (describing the highly revealing nature of CSLI which provides a “detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.”).

115. *Winston v. Lee*, 470 U.S. 753, 766 (1985).

116. *See Sims*, 885 F.3d at 260–63 (finding that a minor’s privacy interests did not diminish to such an extent as to permit a warranted search of his erect penis in a child pornography case).

unconstitutionally violated.¹¹⁷ Accordingly, regardless of whether a neurodata search involves a physical invasion of the body, or whether a valid warrant authorized the neurodata search, the search may nonetheless violate an individual's protections under the Fourth Amendment.

This extension also aligns with the Court's reasoning in *Carpenter*, *Jones*, and *Riley*. If the data at issue in those cases were sufficiently revealing and intimate in nature, as to place that data within the Fourth Amendment's zone of protection, then a neurodata search must fall within its protection as well. But unlike the *Carpenter*, *Jones*, and *Riley* data, all of which the reasonableness determination is assessed under the warrant requirement, the privacy interests with respect to neurodata would likely outweigh any purported government interest, including the government's interest in collecting evidence of a crime.¹¹⁸ And, per *Carpenter*, the third-party doctrine should not apply in cases where highly intimate and revealing data is at issue because the individual does not necessarily lose their privacy expectations even when the data is collected or stored by a third-party.¹¹⁹

Even under the Court's trespass test,¹²⁰ if an individual's home is considered a physical setting that requires a warrant, then it also follows that the individual's brain should be a warrant-required setting because there is no other place or setting where a person can retreat and be free from unreasonable governmental intrusion than his own mind. As the Supreme Court has established, not all trespasses by law enforcement constitute Fourth Amendment violations; the trespass must occur on a "constitutionally protected area—that is, one explicitly enumerated in the text of the Fourth Amendment."¹²¹ Here, the text of the Fourth Amendment is clear; it provides a "right of the people to be secure in their *persons*, houses, papers, and effects"¹²² The plain text of the Fourth Amendment includes the *person*, which

117. *Id.* at 261 ("Although the intrusion suffered by Sims was neither physically invasive nor put him at risk of direct physical harm, the search nonetheless was exceptionally intrusive.")

118. *See* *Winston*, 470 U.S. at 765–66 (holding that because the prosecutor had substantial evidence available, the need for surgery to extract the bullet from the defendant's body was reduced."); *Sims*, 885 F.3d at 262 ("the record demonstrates that there was no evidentiary need to seek a photograph of Sims' erect penis.")

119. *Carpenter*, 138 U.S. at 2219–20 ("There is a world of difference between the limited types of personal information address in *Smith* and *Miller* (the cases that established the third-party doctrine) and the exhaustive chronicle of location information")

120. *See* *Jones*, 565 U.S. at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.") (emphasis in the original).

121. *United States v. Sweeny*, 821 F.3d 893, 900 (7th Cir. 2016) (some quotation marks omitted); *Jardines*, 133 S. Ct. at 1414 (quoting *United States v. Knotts*, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)).

122. U.S. CONST. amend. IV (emphasis added).

logically must include the person's mind.¹²³ Thus, it does not require mental gymnastics to conclude that a person's mind is a "constitutionally protected area" under the plain language of the amendment.

Let us consider the reasonableness determination through a means versus ends lens. Whether a warrantless search is constitutional may, and often does, turn on its proportionality;¹²⁴ were the means taken by the government actor proportional to the end the actor sought? Stated differently, were the means no more intrusive than necessary to achieve the end? While this determination is not dispositive, standing alone,¹²⁵ the intrusiveness of the means to accomplish the end is a weighty factor when assessing the reasonableness of a warrantless search.¹²⁶

Government actions cannot get any more intrusive than a neurodata search (means), no matter the end. Given Fourth Amendment law, and its fundamental principle that an individual must be able to retreat into her own home, one must also be able to retreat into her own mind. This places the privacy of the mind at the most extreme point on a continuum, with privacy in public fora occupying the opposite end. Unlike the home, the government need never pursue a fleeing felon,¹²⁷ prevent the destruction of evidence,¹²⁸ or render emergency aid¹²⁹ into or within an individual's mind. Simply put,

123. See *Katz*, 389 U.S. at 351 ("For the Fourth Amendment protects people, not places."); *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (With respect to a Fourth Amendment violation, "[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security [and] personal liberty . . ."); *Katz & COVID*, *supra* note 18, at 57–58 (assessing the evolution from a physical trespass-centric Fourth Amendment to a person-centric interpretation).

124. See generally *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 643 (1989) (Marshall, J., dissenting) ("[T]he FRA's highly intrusive collection and testing procedures qualify as full-scale personal searches [and accordingly,] a showing of probable cause is therefore clearly required."); *United States v. Curry*, 965 F.3d 313, 354 (4th Cir. 2020) (Richardson, J., dissenting) ("Reasonableness . . . is context specific: attuned to the imminence, probability, and gravity of a threat or exigency, as well as the intrusiveness and effectiveness of the chosen government response.");

125. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995) ("Respondents argue that a 'less intrusive means to the same end' was available . . . [but] [w]e have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."); *Hunsberger v. Wood*, 570 F.3d 546, 556 (4th Cir. 2009) ("[t]he fact that the protection of the public might, in the abstract, have been accomplished by less intrusive means does not, by itself, render the search unreasonable.") (quoting *Cady v. Dombrowski*, 413 U.S. 433, 447 (1973)).

126. *United States v. Lyles*, 910 F.3d 787, 795 (4th Cir. 2018) ("Reasonableness has many dimensions. One must be proportionality between the gravity of the offense and the intrusiveness of the search."); *Cooks*, 920 F.3d at 476 (citing *Mincey*, 437 U.S. at 393); see, e.g., *Wayne v. United States*, 318 F.2d 205, 212 (D.C. Cir. 1963) (describing how courts must take into account the "justification[s] for what would be otherwise illegal absent an exigency or emergency.").

127. See generally *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294 (1967).

128. *King*, 563 U.S. at 462 (2011).

129. See generally *Brigham City, Utah v. Stuart*, 547 U.S. 398 (2006).

neurodata implicates expectations of privacy and interferes with “security of such magnitude” that any intrusion would be unreasonable even if human lives are at stake or a government actor needs to collect evidence of a crime.¹³⁰

III. The Normative Justification for Extending Fourth Amendment Protection to Neurodata

In Part II, I sought to answer *how*, and to some extent, *why* current Fourth Amendment jurisprudence should and must extend to neurodata searches. In Part III, I turn to a normative justification to further argue why the Fourth Amendment should and must extend to neurodata.

A. The Origins of the Fourth Amendment Principles

The Introduction briefly assessed the freedom of thought in the United States. While this individual liberty is often associated with the First Amendment,¹³¹ the history and tradition of the United States support a reading of the Fourth Amendment that includes freedom of thought as well.

Let us begin by turning to the widely recognized history and purpose of the Fourth Amendment. James Madison crafted the Fourth Amendment as a response to the reviled general warrants and writs of assistance of the colonial era, which allowed British officers to arbitrarily search homes in an unrestrained manner.¹³² John Adams later reflected on James Otis’s 1761 speech that condemned writs of assistance, and per Adams, the writs helped spark the revolution itself.¹³³

The Framers rooted the Fourth Amendment’s principles in English common law.¹³⁴ In *Wilkes v. Wood*, Wilkes started a weekly political periodical to counter a pro-governmental publication.¹³⁵ Wilkes’ publication

130. See *Winston*, 470 U.S. at 759 (“A compelled surgical intrusion into an individual’s body for evidence . . . implicates expectations of privacy and security of such magnitude that the intrusion may be unreasonable even if likely to produce evidence of a crime.”).

131. See discussion *supra* INTRODUCTION.

132. Carpenter, 138 S. Ct. at 2213; see generally Jeffrey W. Purcell, *James Otis: “Flame of Fire” Revolutionary Opposing the Writs of Assistance AND Loyal British Subject?*, 5 MASS. LEGAL HIST. 147 (1999) (describing writs of assistance during the colonial era).

133. Purcell, *supra* note 132, at 148 (referencing 10 THE WORKS OF JOHN ADAMS 248 (C. Adams ed. 1856)); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1194, 1250 (2016) (“The War of Independence was fought in part because of the Crown’s effort to exercise writs of assistance, a form of general warrant wherein government officials failed to specify the precise place or person to be searched . . .”).

134. Donohue, *supra* note 133, at 1198; see generally Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869 (1985) (discussing the history of Fourth Amendment jurisprudence and its origins).

135. Donohue, *supra* note 133, at 1199.

vehemently opposed various government actions.¹³⁶ Eventually, Wilkes crossed the line, at least in the eyes of the Earl of Halifax, who directed the King's agents to "make strict and diligent search for the authors, printers, and publishers of a seditious and treasonable paper (Wilkes' publication) [and] seize [them], together with their papers, and to bring in safe custody before [Halifax], to be examined."¹³⁷ Charles Pratt, the Chief Justice of the Common Pleas, ultimately ruled in favor of Wilkes when Wilkes challenged the search and seizure.¹³⁸ Pratt concluded, "Libel being no breach of the peace, the Crown must release Wilkes," and the jury awarded Wilkes £1,000 in damages.¹³⁹

Two years later, in *Entick v. Carrington*, Lord Camden, Chief Justice of the Common Pleas, ruled in favor of Entick, whose house was subjected to a home intrusion using "force and arms."¹⁴⁰ Entick, along with others, launched a weekly paper that "commended good men and censured bad ones."¹⁴¹ The weekly paper ridiculed the political elite at the time, with one elite, the Earl of Halifax, calling it "gross and scandalous."¹⁴² Like in *Wilkes*, Halifax directed King George III's agents to search, obtain, and deliver Entick and his papers to him.¹⁴³ There, Lord Camden recognized that the ultimate offense was not the physical trespass on Entick's property, but rather, it was the "invasion of the indefeasible rights of personal security, liberty, and private property."¹⁴⁴ The wrong occurred as soon as the King's messengers entered Entick's home.¹⁴⁵ Lord Camden also acknowledged that searches and seizures of *papers* specifically could expose an individual's "most valuable secrets" to government scrutiny.¹⁴⁶ Soon after, a chorus of others joined in Lord Camden's sentiment regarding the secrecy and sensitivity of papers.

136. *Id.* at 1200–01.

137. *Id.* at 1201; John Wilkes, *North Briton No. 45*, 2 THE NORTH BRITON 261, 264–65 (1763)

138. Donohue, *supra* note 133, at 1203–04.

139. *Id.*; see Bank of England, *Inflation Calculator*, <https://www.bankofengland.co.uk/monetary-policy/inflation/inflation-calculator> (adjusting for inflation, as of this writing, £1,000 equals £157,010.48 according to the Bank of England).

140. *Entick v. Carrington* (1756) 19 How. St. Tr. 1029, 1066; 95 Eng. Rep. 807); see *Stanford v. State of Tex.*, 379 U.S. 476, 484 (1965) (describing *Entick* as the "wellspring of the rights now protected by the Fourth Amendment . . ."); see also *Coolidge v. New Hampshire*, 403 U.S. 443, 455 n.9 (1971); *Berger v. State of N.Y.*, 388 U.S. 41, 49 (1967) (all Fourth Amendment cases referring to *Entick*).

141. Donohue, *supra* note 133, at 1196.

142. *Id.* at 1197.

143. *Id.*

144. *Id.* at 1198.

145. *Id.*

146. *Entick*, 19 How. St. Tr. at 1064; Schnapper, *supra* note 134, at 882.

Following *Wilkes*, but also applicable to *Entick*, a series of pamphlets addressed the “unprecedented and illegal” seizure of papers in particular.¹⁴⁷ *A Letter to the Right Honorable Earls of Egremont and Halifax, His Majesty’s Principal Secretaries of State, on the Seizure of Papers* complained about the seizure of Wilkes’ papers because such seizures were “of greater importance, or more general concern, as a QUESTION OF LIBERTY, interesting in the highest degree to EVERY SUBJECT in the kingdom.”¹⁴⁸ The *Egremont & Halifax Letter* argued that private papers “often contain an individual’s most private thoughts, never intended to be disclosed to anyone else”¹⁴⁹ Moreover, papers often include confidential communications with others, and the seizure of them acts as a “severe restraint [] laid upon friendship and correspondence, and even upon the *freedom of thought*”¹⁵⁰

Both *Wilkes* and *Entick* served as the foundation for the colonists’ rejection of general warrants and the Framers’ inclusion of the Fourth Amendment protections in the Bill of Rights.¹⁵¹ If these cases, *Wilkes* in particular, and the public responses that followed, were catalytic to the Framers, then they suggest at least some of the Framers’ rationale behind the Fourth Amendment’s protections—protecting the privacy of *thoughts*.¹⁵²

This general respect for the freedom of thought was also captured by the individual colonies (or states). Following these principles promoted by *Wilkes* and *Entick*, States created a positive right to be secure in one’s person, homes, papers, and effects in their state constitutions.¹⁵³ For example, while technically separate from Virginia’s 1776 Constitution, its Declaration of Rights, passed days before its constitution, affirmatively captured the colonists’ sentiment at the time: the elevation of sovereign reason, thought,

147. Schnapper, *supra* note 134, at 889.

148. *Id.*; *Letter* (London 1763) at 56 (emphasis in the original) [hereinafter *Egremont & Halifax Letter*].

149. Schnapper, *supra* note 134, at 890; see *Egremont & Halifax Letter*, *supra* note 148, at 8–9.

150. *Egremont & Halifax Letter*, *supra* note 148, at 2531 (emphasis added).

151. Donohue, *supra* note 133, at 1196; These cases also served as a basis for Sir Edward Coke’s proclamation that “a man’s home is his castle”—deserving of some form of privacy protection. In *Semayne’s Case* (1604) 5 Coke Rep. 91, Coke wrote, “the house of every one is to him as his . . . castle and fortress.” In other writings, Coke proclaimed, “*domus sua cuique est tutissimum refugium*,” meaning “each man’s home is his safest refuge.”

152. Schnapper, *supra* note 134, at 910, 912 (“These pamphlets, speeches, and public letters played an important role in shaping public opinion on both sides of the Atlantic. . . . These rights sprang from the same tradition of individual liberty that led to the federal Bill of Rights in America.”).

153. See, e.g., VA. CONST. OF 1776 (The state of Virginia’s first constitution enshrined the Virginia Declaration of Rights).

consciousness, and ideas.¹⁵⁴ As sovereign reason, thought, consciousness, and ideas elevated amongst the colonists, even before Virginia captured it in its constitution and Declaration of Rights in 1776, the colonies inched closer to the Declaration of Independence and revolution.¹⁵⁵ But it was perhaps Thomas Paine who best captured the Revolution as a revolution of intellect, reason, and thought.¹⁵⁶ Paine proclaimed that the revolution rejected tyranny, and most importantly, the *tyranny of men's minds*.¹⁵⁷ “Mankind are not now to be told they shall not think, or they shall not read; and the publications that go no farther than to investigate principles of government, to invite men to reason and to reflect, and to show the errors and excellences of different systems, have a right to appear,” Paine declared.¹⁵⁸

Certainly, the Earl of Halifax sought to quash the publications in *Wilkes* and *Entick*—both of which were rooted in criticism of the Crown and his agents. In a way, these cases, subsequent publications, and the public discourse that followed acted as a row of dominoes—falling one at a time, one leading to another to set off the Revolution of intellect, reason, and thought. And the principles embodied in the Fourth Amendment reflect how protecting “persons, houses, papers, and effects,” vitally protects the freedom of thought.

Thus, the Fourth Amendment is historically rooted in the freedoms of intellect and thought and the rights to contemplate and reason. Said differently, the Fourth Amendment protects an individual’s thoughts from unreasonable revelation to the government. While in the 1700s, the revelation stemmed from papers often found in the home, it follows that a digital form of thoughts—neurodata—falls squarely within the Fourth Amendment’s historical purpose.

B. Moral Reasoning

In Part II.C, I argued that government cannot get any more intrusive than a neurodata search no matter the end—not even to solve or prevent

154. At its Convention of 1776, Virginia adopted its Declaration of Rights on June 12, 1776, and shortly thereafter on June 29, 1776, it adopted its first Constitution; see *The Virginia Declaration of Rights*, NAT’L ARCHIVES (Sept. 26, 2016), <https://www.archives.gov/founding-docs/virginia-declaration-of-rights>; Wayne Unger, *Stay Out of My Head: Neurodata, Privacy, and the First Amendment*, WASH. & LEE L. REV. (forthcoming 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4293432# (detailing how pamphlets and other writings were critical in transforming people’s minds, beliefs, and sensibilities and sparking an intellectual and moral revolution rooted in free thought and consciousness).

155. C. BRADLEY THOMPSON, *AMERICA’S REVOLUTIONARY MIND: A MORAL HISTORY OF THE AMERICAN REVOLUTION AND THE DECLARATION THAT DEFINED IT* 45 (2019).

156. *Id.* at 44.

157. See Thomas Paine, *Rights of Man, Part the Second*, in *LIFE AND WORKS OF PAINE*, 6:225-26, 231 (1792).

158. *Id.*

crimes.¹⁵⁹ Not only are there legal and normative justifications for this assertion, there is also a moral justification. The moral justification for protecting neurodata from government intrusion is, at least in part, aligned with the fundamental proposition in criminal law: judicial punishment ought not to be inflicted for private thoughts.¹⁶⁰

It is a widely accepted and unquestionable maxim of criminal jurisprudence that the state must never punish an individual for their mere thoughts.¹⁶¹ One rationale for this maxim is that mere thoughts cannot be proved beyond a reasonable doubt.¹⁶² William Blackstone wrote, “no temporal tribunal can search the heart, or fathom the intentions of the mind, otherwise than as they are demonstrated by outward actions, it therefore cannot punish for what it cannot know.”¹⁶³ In other words, if a thought or intention is unprovable, then it must also be unpunishable, unless it can be shown via expressive evidence.¹⁶⁴ However, in a future state where brain-computer interfaces and neurodata are more ubiquitous, then almost certainly, mere thoughts could be provable before a tribunal.

From a public policy perspective, surely the maxim is intrinsically tied to the freedom of expression and the marketplace of ideas.¹⁶⁵ Perhaps this tie arises from the potential chilling effect on thought itself. John Stuart Mill argued, “the peculiar evil of silencing the expression of an opinion is, that it is robbing the human race . . . those who dissent from opinion, still more than those who hold it.”¹⁶⁶ Further, Justice Holmes asserted that “the best test of truth is the power of the thought to get itself accepted in the competition of the market”¹⁶⁷ But neither Mill nor Justice Holmes captured a wrong on the speaker; rather, they captured the wrong onto society.¹⁶⁸ So, what is the potential harm to the speaker with respect to the maxim that mere thoughts ought not to be punished?

159. See *supra* note 115, accompanying text, and surrounding arguments.

160. ALAN BRUDNER, PUNISHMENT AND FREEDOM: A LIBERAL THEORY OF PENAL JUSTICE 108 (2009).

161. Gabriel S. Mendlow, *Why Is It Wrong to Punish Thought?*, 127 YALE L. REV. 2342, 2345 (2018).

162. *Id.* at 2354; 2 SIR JAMES FITZJAMES STEPHEN, A HISTORY OF THE CRIMINAL LAW OF ENGLAND 78 (1883). Another rationale, for example, is the harm principle from John Stuart Mill. The harm principle is based on the principle that harm onto others is punishable, but as in the case of mere thoughts where harm is minimal or in-existent, mere thoughts cannot be punishable.

163. 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, CH. 2 (1769).

164. Mendlow, *supra* note 161, at 2356 (“Unexecuted intentions instead must be proved from *expressive evidence*, such as a person’s self-reports. . . . [E]xpressive evidence is arguably the superior form [compared to executory evidence].”).

165. See *id.* at 2361.

166. JOHN STUART MILL, ON LIBERTY 16 (1859).

167. *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

168. Mendlow, *supra* note 161, at 2361.

Professor Gabriel Mendlow posited that the maxim—“punishing mere thoughts is categorically impermissible”—is entrenched in the unjust violation of a personal right to mental integrity.¹⁶⁹ In other words, the notion that it is unjust to punish mere thoughts stems from the rejection of “direct and forcible intrusion into the mind,” or as Mendlow characterizes it, “direct and forcible mind control.”¹⁷⁰ This right to mental integrity, quite simply, means a right “to be free from unwanted mental interference or manipulation.”¹⁷¹ And the right to mental integrity is a fundamental right that society has already accepted as true.¹⁷²

Take *Stanley v. Georgia* as an example.¹⁷³ In that case, the Supreme Court held that the state cannot penalize the mere possession of obscene materials.¹⁷⁴ The Court based its holding in “[o]ur whole constitutional heritage rebels at the thought of giving government the power to control men’s minds.”¹⁷⁵ In so holding, the Court also rejected Georgia’s argument that it had a “right to control the moral content of a person’s thoughts.”¹⁷⁶ The *Stanley* Court endorsed the right to mental integrity, and illustrated that the harm in penalizing mere thoughts relates to the right of mental integrity and an independent and free mind.

Thus, the moral justification for not penalizing mere thoughts conceivably ties to the potential harm to the speaker—that is, a societal rejection of controlling an individual’s thoughts and manipulating one’s mind. The Court best captured this societal rejection in *West Virginia State Board of Education v. Barnette*. The Court declared, “[i]f there is any fixed star in our

169. *Id.* at 2368.

170. *Id.*

171. *Id.*

172. See, e.g., *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 253–54 (2002) (holding that a state cannot penalize visual depictions of actors who appear to be minors engaging in sexual intercourse because, unlike real child pornography where the compelling government interest is to protect the child depicted, penalizing simulated child pornography holds no such interest as the penalization is merely for controlling the effect of the viewer’s mind); *Martin v. City of Struthers, Ohio*, 319 U.S. 141, 149 (1943) (Murphy, J., concurring) (noting that the right to a free mind and the right to believe as one chooses are “essential to enlightened opinion and right conduct on the part of the citizens of a democracy.”); *United States v. Reidel*, 402 U.S. 351, 356 (1971) (“The focus of [‘Our whole constitutional heritage rebels at the thought of giving government the power to control men’s minds’] was on freedom of mind and thought and on the privacy of one’s home.”); *Rennie v. Klein*, 462 F. Supp. 1131, 1144 (D.N.J. 1978) (stating that the constitutional right to privacy inherently includes the freedom of thought and the right to protect one’s mental processes from governmental intrusion and interference).

173. See generally 394 U.S. 557 (1969).

174. *Id.* at 559.

175. *Id.* at 565.

176. *Id.*

constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox . . . or other matters of opinion”¹⁷⁷

Conclusion

For over two centuries, the Fourth Amendment has protected individuals against unreasonable government intrusion. But government intrusion itself has evolved since the Fourth Amendment’s ratification. Once prolific in general warrants and writs of assistance, the methods of intrusion have changed as technology has advanced. Justice Brandeis most famously recognized technology’s impact when he proclaimed, “[t]ime works changes, brings into existence new conditions and purposes” for which civil rights are meant to protect.¹⁷⁸ As he argued, the Fourth Amendment in particular “must be capable of wider application than the mischief which gave it birth.”¹⁷⁹

In general, Fourth Amendment jurisprudence has heeded Justice Brandeis’ philosophy. The 20th Century brought rapid advancement in technology, and “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”¹⁸⁰ *Carpenter* recognized the sensitivity and intimacy of voluminous autogenerated data that can reveal a data subject’s most intimate associations, secrets, and beliefs.¹⁸¹ *Riley* acknowledged that law enforcement cannot arbitrarily search personal data.¹⁸² And other cases, like *Sanchez*, illustrate the potential harms of invasive searches of one’s body.¹⁸³

The next frontier of privacy risks and invasive government action is emerging, and it presents a battle for your brain.¹⁸⁴ Neurodata will be the last stand for personal privacy; if one cannot retreat into their own mind without the fear or practice of government intrusion, then privacy will cease to exist. One must be able to keep their own thoughts, ideas, and beliefs secret. Just as the Fourth Amendment has protected individual privacy for decades, so too should it protect the individual’s mind.

As this Essay has argued, the Fourth Amendment’s origins and jurisprudence support a logical extension of its protections to neurodata. Its origins are rooted in protecting individuals’ thoughts from unreasonable revelation to the government. Jurisprudentially, the Fourth Amendment protects

177. *W. Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624, 642 (1943).

178. *Olmstead v. United States*, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting).

179. *Id.* at 473.

180. *Kyllo*, 533 U.S. at 33–34.

181. *See* discussion *supra* Part II.A.

182. *See id.*

183. *See* discussion *supra* Part II.B.

184. *See generally* FARAHANY, *supra* note 21.

people, their bodily autonomy, and their protected areas—all of which are extendable to neurodata. But perhaps at the most fundamental level, the Fourth Amendment ought to extend to protect neurodata because the converse would run afoul of the societal rejection of controlling an individual's thoughts and manipulating the mind.

As Thomas Paine advocated, America's revolution from King George III rejected tyranny, including the tyranny of men's minds.¹⁸⁵ And if there is any conceivable basis for precluding the government from accessing or intruding upon neurodata, it is because “[t]o lose freedom of thought is to lose our dignity, our democracy and our very selves.”¹⁸⁶

185. Paine, *supra* note 156.

186. Simon McCarthy-Jones, *The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century*, 2 FRONTIERS IN ARTIFICIAL INTELLIGENCE 19 (Sept. 26, 2019).