NOTE

NEUROSEARCHES

Josh A. Roth†

Neurotechnology is advancing exponentially, and the laws of data privacy and security cannot keep pace. Soon, governments will exploit this technology in criminal investigations with what this Note calls "neurosearches." Scholars have argued against the compelled gathering of neurological evidence as a violation of the Fifth Amendment, likening it to testimony and thus barred as self-incrimination. But no court has said so explicitly.

This Note operates under the premise that compelled gathering of brain data survives a Fifth Amendment challenge and evaluates these neurosearches under the Fourth Amendment. Part I of this Note summarizes the contemporary state of neuroscience in the commercial marketplace and in the eyes of the law. Part II outlines the Supreme Court's Fourth Amendment jurisprudence, detailing its application to technologically advanced searches. Part III contemplates the disposition of challenges to neurosearches based on the jurisprudence described in Part II.

This Note ultimately concludes that compulsory searches for proprietary brain data survive the reasonableness and particularity requirements of the Fourth Amendment and that commercial brain data falls within the third-party doctrine.

† Josh A. Roth is a student at Cornell Law School and an Articles Editor for the *Cornell Law Review*.

> "We are past due on the urgent need to recognize the right to cognitive liberty over our brains and mental experiences."
> –Nita A. Farahany[1]

> "Cognitive warfare represents the convergence of all the elements of 'information warfare' expanded by operational notions of psychology and neuroscience[.]"
> –François du Cluzel[2]

INTRODUCTION

In 2012, bioethicist and Professor of Law Nita Farahany published two law review articles conceptualizing government exploitation of neurotechnology.[3] Since then, the Supreme Court's treatment of the Fourth Amendment has significantly evolved, and neuroscience has improved exponentially. Farahany's articles left open the question to which this Note offers a modern answer: whether government searches of brain data — neurosearches — would survive constitutional scrutiny under the Fourth Amendment.

Part I of this Note summarizes the contemporary state of neuroscience in the commercial marketplace and in the eyes of the law. Part II outlines the Supreme Court's Fourth Amendment jurisprudence, detailing its application to technologically advanced searches. Part III contemplates the disposition of various challenges to neurosearches based on the jurisprudence described in Part II.

---

1 NITA A. FARAHANY, THE BATTLE FOR YOUR BRAIN: DEFENDING THE RIGHT TO THINK FREELY IN THE AGE OF NEUROTECHNOLOGY 214 (2023).

2 François du Cluzel, *Cognitive Warfare, a Battle for the Brain*, N. ATL. TREATY ORG. (2020). While not the focus of this Note, there are countless national security concerns that arise from the continued evolution of neurotechnology. For a qualitative analysis of these concerns, *see generally* Joseph DeFranco, Maureen Rhemann, & James Giordano, *The Emerging Neurobioeconomy: Implications for National Security*, 18 HEALTH SEC. 267 (2020).

3 Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239 (2012) [hereinafter Farahany, *Searching Secrets*] (hypothesizing how the Fourth Amendment applies to emerging technology with respect to neuroscience); Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351 (2012) [hereinafter Farahany, *Incriminating Thoughts*] (criticizing the testimonial-physical dichotomy of evidence by considering neurological evidence).

I
THE BASICS OF BRAIN DATA

Electroencephalograms (EEG) measure bioelectrical brain waves in cycles per second, or hertz (Hz).[4] The four classifications of these waves are "delta waves" (0–4 Hz), "theta waves" (4–8 Hz), "alpha waves" (8–13 Hz), and "beta waves" (13–20 Hz).[5] Other complex brain waves, such as the P300,[6] may measure the transfer of information to consciousness, reflecting "positive deflection" in event-related potential.[7] Neuroscientists analyze the occurrence, frequency, and volatility of these brain waves for various reasons. For instance, because the brain cycles less electricity while unconscious, delta waves predominantly occur during sleep.[8] So a gradual decrease in beta waves, coupled with an increase in theta waves, could reasonably be translated to the early stages of drowsiness.[9] The corollary would be a gradual decrease in theta waves with an increase in delta waves, reflecting sleep.[10] This now-rudimentary monitoring of brain data has been used by employers in transportation, excavation, and construction industries to monitor employee fatigue to mitigate liability for injuries.[11] But today, brain data reveals much more than tiredness. Modern neurotech can show a subject's focus (including what kind of task the subject is focused on),[12] signs of deception,[13] and even recreate mental images.[14]

---

4 Gregory Xavier, Anselm Su Ting & Norsiah Fauzan, *Exploratory Study of Brain Waves and Corresponding Brain Regions of Fatigue On-Call Doctors Using Quantitative Electroencephalogram*, J. OCCUPATIONAL HEALTH 1, 2 (2020).

5 *Id.*

6 P300 refers to electrical responses by the brain within 300 milliseconds after exposure to a stimulus. Alexandra J. Roberts, *Everything New is Old Again: Brain Fingerprinting and Evidentiary Analogy*, 9 YALE J.L. & TECH. 234, 258 (2007).

7 Terence W. Picton, *The P300 Wave of the Human Event-Related Potential*, 9 J. CLINICAL NEUROPHYSIOLOGY 456, 456 (1992).

8 Xavier, Ting, & Fauzan, *supra* note 4, at 2.

9 *Id.*

10 *Id.*

11 FARAHANY, *supra* note 1, at 40–41. *See also* Peter Ker, *Australian Employers are Scanning Their Workers' Minds*, AUSTL. FIN. REV. (Jul. 3, 2015). Recently, even the U.S. Department of Justice has acknowledged the benefits of using neuroscience to measure stress in correction officers. Eric Martin, *Emerging Relevance of Neuroscience in Corrections*, U.S. DEP'T OF JUST., NAT'L INST. OF JUST. (Mar. 6, 2023).

12 FARAHANY, *supra* note 1, at 48–49.

13 *Id.* at 79–80.

14 Guohua Shen, Tomoyasu Horikawa, Kei Majima & Yukiyasu Kamitani, *Deep Image Reconstruction from Human Brain Activity*, PLOS COMPUTATIONAL BIOLOGY (2019).

A. Categories of Data

In arguing that neurological evidence can be testimonial and thus barred under the Fifth Amendment, Farahany qualified the spectrum of neuroscientific evidence into four discrete categories: identifying, automatic, memorialized, and uttered.[15] These categories are also relevant to an analysis of searching for neurological evidence under the Fourth Amendment.

Identifying evidence (neurological or not) narrows down a suspect pool; it includes basic data like name and date of birth, but also extends to physical characteristics such as height, weight, shoe size, blood type, or DNA.[16] As the name suggests, "identifying" brain data (e.g., wave data and static images of a person's brain) can reveal identifying information relevant to a criminal investigation, not unlike fingerprints.[17] Farahany proffers an example of a suspect to an assault who suffered a defensive strike to the head. Investigators who executed a warrant for a structural neuroimage of the suspect could then discover brain abnormalities or brain damage, thus corroborating or refuting the victim's statement.[18]

Automatic evidence includes what occurs with little conscious control by the individual, incorporating the autonomic nervous system.[19] Breathing, blinking, or sexual arousal, for example, all fall in this category. Investigators could compel a suspect to undergo a positron emission tomography (PET scan) to measure the suspect's brain's reactions to various stimuli, such as being presented with photographs of a victim's face.[20] But research shows it can also detect subconscious recognitions of that stimulus (e.g., without the subject affirmatively recognizing the stimuli).[21] This visceral reaction can be analyzed as a change in the suspect's emotional state. Neuroscience researchers Marco Tamietto & Beatrice de Gelder stated the "non-conscious perception of visual stimuli" shows

---

15 Farahany, *Incriminating Thoughts*, *supra* note 3, at, 366–400.

16 *Id.* at 366–68.

17 *Id.* at 368.

18 *Id.* at 368–69.

19 *Id.* at 372–73.

20 *See* Stacey A. Tovino, *Imaging Body Structure and Mapping Brain Function: A Historical Approach*, 33 AM. J.L. & MED. 193, 212–13 (2007). As Farahany points out, this kind of evidence muddies the waters of the testimonial/physical dichotomy and thus raises constitutional questions under the Fifth Amendment. *See generally* Farahany, *Incriminating Thoughts*, *supra* note 3, at 351. This Note assumes *arguendo* that automatic brain data is physical and thus subject to equal Fourth Amendment scrutiny as identifying brain data.

21 Farahany, *Incriminating Thoughts*, *supra* note 3, at 384.

a quantifiable change in emotional state based on neurophysiological responses.[22] So instead of a cumbersome PET scan, savvy investigators could present a suspect with photographs of a victim outside his zone of conscious awareness, yet still acquire the automatic brain data associated with his response.

Memorialized evidence is what is recorded separate from the author; emails, bank records, and Jeffrey Epstein's "black book" all fit the archetype.[23] Farahany extends this definition to include data recorded (encoded) in the brain as memories.[24] A Stanford University study suggests that when presented with familiar stimuli, a subject's brain "recognizes" it and the response can be measured via functional MRI (fMRI) and multivariate data analysis.[25] Thus, police could present a suspect with details relevant to the investigation, hidden from the public, and determine whether he "recognizes" the detail.[26] This capability transcends minute details; neurotech can now detect episodic memories. Farahany calls this a collection of "the neural representations of the autobiographical details experienced in everyday life, including the substantive content and the geographic, spatial, and temporal orientation of those experiences."[27]

Uttered evidence is the personal interpretation of thoughts and memories, brought from the subconscious mind into reality.[28] Obvious self-incrimination issues arise depending on whether orally uttered evidence was voluntary or compelled. But utterances of the brain are not verbal, muddying the waters of the physical-testimonial dichotomy.[29]

B. Commercial Neurotechnology

Experts predict that by 2026, the neurotechnology industry will be worth over $20 billion.[30] Existing companies and their products provide key insight into the kinds of data already being collected, foreshadowing law enforcement exploitation.

---

22 Marco Tamietto & Beatrice de Gelder, *Neural Bases of the Non-Conscious Perception of Emotional Signals*, 11 NATURE REV. NEUROSCIENCE 697, 697 (2010).

23 *See* Farahany, *Incriminating Thoughts*, *supra* note 3, at 379.

24 *Id.*

25 Jesse Rissman, Henry T. Greely & Anthony D. Wagner, *Detecting Individual Memories Through the Neural Decoding of Memory States and Past Experience*, 107 PROC. NAT'L ACAD. SCI. 9849, 9849 (2010).

26 Farahany, *Incriminating Thoughts*, *supra* note 3, at 379–80.

27 *Id.* at 383.

28 *Id.* at 389.

29 *See generally id.* at 389–400.

30 Nita A. Farahany, *Neurotech at Work*, HARV. BUS. REV. (Mar. – Apr. 2023).

Bryan Johnson owns Kernel, a company originally formed to fabricate memory prosthesis — essentially a neural external hard drive to transfer, store, and organize human memories in the host's hippocampus.[31] Now, Kernal aims to use that technology for clinical diagnoses such as Alzheimer's.[32] Elon Musk has more ambitious plans with Neuralink, a company that aims to produce implants that directly link a human brain to a computer.[33] Musk envisions a future where "superhuman cognition" is a widely available product.[34] The core issue with products such as those offered by Musk and Johnson is palatability by the public.[35] But two companies, EMOTIV and CTRL-Labs, approach neurotech with devices that easily integrate into common gadgets.

EMOTIV developed the MN8, a Bluetooth headset with EEG sensors incorporated.[36] Like SmartCaps used in trucking and construction,[37] the MN8 measures changes in stress, attention, productivity, and alerts the user to potential health issues.[38] The MN8 operates in all the same ways Apple's AirPods do and looks like a pair of Bose SoundSport headphones. EMOTIV has stirred controversy in its marketing of the MN8; it offers them to employers to surveil employees.[39]

CTRL-Labs fabricated a device that defies the common factor in products made by Kernal, Neuralink, and EMOTIV. Those products all require intrusions into the user's head (e.g., a headset or neural implant). But CTRL-Labs, now owned by Facebook's parent company, Meta, created a wristband that can gather, encode, and analyze brain data.[40] The technology is suitable for addition into a smartwatch, allowing for

---

31 CB INSIGHTS, *21 Neurotech Startups to Watch: Brain-Machine Interfaces, Implantables, and Neuroprosthetics* (Jan. 28, 2019), https://www.cbinsights.com/research/neurotech-startups-to-watch/ [https://perma.cc/THL9-KYWN].

32 *Id.*

33 *Id.*

34 *Id.*

35 FARAHANY, *supra* note 1, at 15–16 (discussing how contemporary commercial neurotech was "unlikely to motivate people to go about their everyday lives wearing a silly-looking headband.").

36 EMOTIV,https://www.emotiv.com/workplace-wellness-safety-and-productivity-mn8/ [https://perma.cc/MM5W-EKDM] (last visited Mar. 20, 2023).

37 *See* Ker, *supra* note 11 and accompanying text.

38 EMOTIV, *supra* note 36.

39 FARAHANY, *supra* note 1, at 48. *See also id.* at 26–31 (documenting how other companies, such as Ikea and Tesco, have implemented commercial neurotechnology and capitalized on brain data).

40 *Id.* at 30–31 ("While . . . CTRL-labs' EMG device collects information locally, at muscle junctures rather than the brain, EMG data is no less sensitive than raw brain data.").

seamless social integration. In fact, Meta has admitted it intends to incorporate the neural wristbands in future releases of its smartwatch.[41]

The issues posed by commercial neurotech are twofold. First, the collection of data relies on consent by the user. This barrier to investigator's collection of a suspect's brain data exists until employment depends on consent to using devices such as the MN8 or Meta EMG wristband.[42] Second, as discussed below, the law does little (if anything) to protect the public against exploitation of this data.

C. Neuroethics and the Law

No U.S. statute protects citizens against the government exploitation of neurotechnology in criminal investigations. In fact, the law does little to protect from abuse of neurotechnology generally, whether by private or public actors. Esther Shein recently discussed several dangers posed by the exponential advancement of neurotechnology — addiction, brain damage, or hacking, for example — without any regulation.[43] Rajesh P.N. Rao also cautioned that brain data could be intercepted by "criminals, terrorists, commercial enterprises, or spy agencies as well as legal, *law enforcement*, and military entities."[44]

Internationally, the contemporary data privacy laws and regulations theoretically apply, but in practice do little to limit the exploitation of personal data. The European General Data Protection Regulation (GDPR), for instance, merely requires that employers have a "legitimate basis" (e.g., public welfare, employee safety, or increasing productivity) for collecting the data.[45]

Dr. Spyridon Orestis Palermos proffers an approach to integrating brain data into the current data privacy infrastructure. He argues that the existing dichotomy — data and metadata —

---

41 Tommy Palladino, *Facebook's Smartwatch Will Eventually Include CTRL-Labs Tech for Smartglasses Control, Report Says*, NEXT REALITY (Jun. 9, 2021), https://next.reality.news/news/facebooks-smartwatch-will-eventually-include-ctrl-labs-tech-for-smartglasses-control-report-says-0384724/ [https://perma.cc/9ZSW-ZPAU].

42 This type of surveillance dynamic existed for employees of the U.K. chain Tesco, who were forced to wear armbands that tracked productivity and movement. *See* FARAHANY, *supra* note 1, at 41–43.

43 Esther Shein, *Neurotechnology and the Law*, 65 COMMC'N OF THE ACM 16, 18 (2022).

44 Rajesh P. N. Rao, *Brain Co-Processors: Using AI to Restore and Augment Brain Function*, HANDBOOK OF NEUROENGINEERING, (2021) (emphasis added).

45 2016 O.J. (L 119) 7–8.

does not suitably incorporate neuroscientific data, and thus a third category — mental data — must be independently qualified.[46] In accepting Clark & Chalmers' Extended Mind Thesis,[47] Palermos suggests that when executing mental tasks assisted by technology (scheduling in a calendar, organizing photographs, recalling autobiographical information for notes), agents bidirectionally interact with artifacts and integrate.[48] Thus, such information is neither exclusively data nor metadata but an extension of the user's mind — mental data.[49] In 2014, The U.N. was concerned with how states can use this kind of data and cautioned against surveillance as a potential human rights violation:

> *Noting* that while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity,
>
> *Emphasizing* that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken on a mass scale[.][50]

The distinction between data, metadata, and mental data does not dispose of any legal argument surrounding its use in criminal investigations. But it does suggest that, because of the substantial overlap, the caselaw on cybersecurity and exploitation of cyberspace help explain how a court may wrangle with neurotechnology in criminal investigations.

II
The Current State of Affairs: The Fourth Amendment and Technologically Advanced Searches

The Fourth Amendment safeguards a person's security in "their persons, houses, papers, and effects, against unreasonable searches and seizures[.]"[51] The primary mechanism securing this interest is the constitutional requirement of a search

---

46 Spyridon Orestis Palermos, *Data, Metadata, Mental Data? Privacy and the Extended Mind*, Am. J. Bio. Neuroscience 1, 1 (2022).

47 Andy Clark & David Chalmers, *The Extended Mind*, 58 Analysis 7, 7 (1998).

48 Palermos, *supra* note 46, at 3–4.

49 *Id.* at 1.

50 G.A. Res. 69/166, ¶¶ 14–15 (Dec. 18, 2014).

51 U.S. Const. amend. IV.

or seizure warrant supported by probable cause, that describes in particularity the place to be searched or the person/property seized.[52] Central to any Fourth Amendment challenge is standing; that is, whether the government invaded "the security a man relies upon when he places himself or his property within a constitutionally protected area."[53] Of course, the Constitution is hundreds of years old; those who wrote it never conceptualized how police would employ modern technology to conduct searches and seizures. Despite this, traditional Fourth Amendment principles have been applied to searches executed with advanced technology.[54]

The exploitation of neurotechnology in criminal investigations requires a search of the body (brain) with advanced technology. No court has yet to rule on the constitutionality or even evaluate a search warrant request for neurotech in investigations. That said, the technology is evolving exponentially, inching toward that reality. To predict an evaluation of it, this section summarizes the current jurisprudence on government searches of the body and cyberspace with advanced technology.

A. Exploiting Advanced Technology in Government Searches

In *Katz v. United States*, the Supreme Court somewhat revolutionized the Fourth Amendment's protections, holding that any place in which a person justifiably relied on privacy was a constitutionally protected area.[55] The Court held that FBI agents violated a defendant's Fourth Amendment rights after recording his conversation inside a public telephone booth without his consent or knowledge.[56] Although somewhat ambiguous at the time, *Katz* was not a re-write of the Fourth Amendment, which had traditionally applied to physical intrusions akin to trespass. But in *United States v. Jones*, the Supreme Court revived the property-based theory, clarifying that *Katz* supplemented, not replaced, this trespass principle.[57] To counter the

---

52 *Id.*

53 United States v. Miller, 425 U.S. 435, 440 (1976) (quoting Hoffa v. United States, 385 U.S. 293, 301–02 (1996)).

54 *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967) (pen register used to record conversation in public phone booth); Kyllo v. United States, 533 U.S. 27 (2001) (thermal-imaging equipment used to identify drug activity in private housing); Carpenter v. United States, 138 S. Ct. 2206 (2018) (geolocation data derived from cell towers used to track defendant's movements).

55 *Katz*, 389 U.S. at 353.

56 *Id.*

57 United States v. Jones, 565 U.S. 400, 405–07 (2012).

popular attack by originalist Justices and scholars that *Katz* was wrongly decided, Professor Orin S. Kerr offers a theory that *Katz* is consistent with originalist (textualist) ideology.[58] A textualist, says Kerr, asks four questions in a Fourth Amendment challenge: (1) is the item a person, house, paper, or effect?; (2) if so, was the item searched or seized?; (3) if so, was the item that was searched or seized that person's house, paper, or effect?; and (4) if so, was the search or seizure unreasonable?[59] And when contrasted with Justice Harlan's concurring opinion in *Katz* (which established the ubiquitous reasonable expectation of privacy test), it appears Justice Harlan employed those four questions.[60] Further supporting this textualist reading of *Katz* is Justice Scalia's criticism of *Katz* in *Jones*, while the two cases were ultimately similar in outcome.[61]

Given this relationship, one must then reconcile *Jones* with *United States v. Knotts*.[62] To do so, one must acknowledge that it is not the *characteristics* of the data recovered that render an act a search; rather, it is the *means* by which the police obtain the data. Put simply, police acquisition of GPS data is not a search per se.[63]

Fourth Amendment scholars routinely emphasize the unique protections enjoyed by private citizens in their homes, a principle also derived from an originalist interpretation of the Constitution. Criminal procedure professor Thomas Y. Davies described the origins of the Fourth Amendment's protections as having been "almost exclusively about revenue searches of houses under general warrants."[64] But even before

---

58 Orin S. Kerr, *Katz as Originalism*, 71 DUKE L. J. 1047, 1084 (2022).

59 *Id.* at 1052.

60 *Id.* at 1053–54. (citing *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring)).

61 *Id.* at 1085–88.

62 United States v. Knotts, 460 U.S. 276, 285 (1983) (upholding a search when police put a beeper that tracked location information into a bottle of chloroform that was given to the defendant).

63 For a deeper discussion on the means used as dispositive for the reasonable expectation of privacy test, see Josh A. Roth, *Drawing Lines: Geofence Warrants and the Third-Party Doctrine*, 4 INT'L CYBERSECURITY L. REV. 213, 221–22 (2023). The majority in *Knotts* articulated this principle as a matter of scientific enhancement of the senses. 460 U.S. at 282, 285 ("Nothing in the Fourth Amendment prohibited the police from augmenting the[ir] sensory faculties . . . with such enhancement as science and technology afforded them in this case. . . . [T]here is no indication that the beeper was used in any way to reveal information as to the movement of the [chloroform container] within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin. . . .").

64 Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 553 (1999).

investigators began exploiting cyberspace, there were plenty of technologically advanced methods to surveil a suspect without violating the Fourth Amendment, even within the privacy of their home. This permissive intrusion already suggests that searching for brain data is within the realm of possibility, as the home was the pinnacle of Fourth Amendment protection. These cases, namely *Ciraolo* and *Riley*, reflect a simple principle: use of advanced technology by police, even if used to surveil into a home, is not a search within the meaning of the Fourth Amendment so long as the technology used is within the public sphere.[65] *Ciraolo* and *Riley* validated warrantless aerial surveillance, by plane and helicopter, respectively.[66] But these cases were used by the court in *Kyllo* to invalidate warrantless use of thermal imaging cameras to reveal a defendant's drug-growth operation.[67]

B. Searching the Body

Judges routinely consider and approve searches for DNA, blood, fingerprints, and compelling a suspect to submit to a sexual assault forensic examination (SAFE). As discussed below, the common concern is not the revealing nature of the data searched, but the physical intrusion into the suspect's body.

In *Maryland v. King*, the Supreme Court held that collection of DNA was a reasonable search under the Fourth Amendment as a routine police booking procedure.[68] Justice Kennedy described DNA technology as "one of the most significant scientific advancements of our era."[69] He described how even a suspect who undergoes reconstructive surgery to evade photographic identification, or alters his fingerprints, cannot "escape the revealing power of his DNA."[70] Even so, the Court found that the collection of DNA through a cheek swab was a "minimal" intrusion and affirmed the State's methods of DNA collection and exploitation.[71] The Court similarly affirmed

---

65 Roth, *supra* note 63, at 222–23 (discussing California v. Ciraolo, 476 U.S. 207 (1968) and Florida v. Riley, 488 U.S. 445 (1989)).

66 *Id.* at 223.

67 Kyllo v. United States, 533 U.S. 27, 29–30 (2001). For a deeper discussion on the relationship between *Ciraolo*, *Riley*, and *Kyllo* and the evolving application of the "public sphere" rule, *see* Roth, *supra* note 63, at 222–23.

68 Maryland v. King, 569 U.S. 435, 465 (2013).

69 *Id.* at 442.

70 *Id.* at 459.

71 *Id.* at 463.

police exploitation of blood draws,[72] fingernail scrapings,[73] and breathalyzers.[74]

Requiring a suspect to submit to a SAFE incident to arrest maximizes physical invasiveness. In executing the SAFE, nurses (as an agent of the government) search for bodily secretions, blood, urine, stains, foreign objects, fingernails, pubic hair samples/combings, semen, saliva, buccal swabs, anal swabs, and photographic evidence of the suspect's naked body.[75] Yet given the stakes involved in sex crime investigations, warrants for these searches are routinely granted.

C. Searching Cyberspace

I begin this section by summarizing the technical terms used within. Definitions vary by jurisdiction, but generally, geolocation data reflects information from electronic devices that depicts the location of an individual or device, whether retroactively, presently, or in the future.[76] Cell site location information (CSLI) is the geolocation data generated when a mobile phone connects to a cell tower, retained by the wireless carrier.[77] Smaller cell site coverage correlates to more precise geolocation data of the specific user.[78] With increased prevalence of cell phones follows an increased number of cell towers, resulting in more precise locations identified by CSLI.[79] One exploitation of cell towers is a "tower dump," whereby police receive a record of each individual device that connected to a particular tower during a specified period.[80] Tower dumping evolved into geofencing, which is essentially a towerless tower dump; that is, a geofence identifies every device encapsulated

---

72 Schmerber v. California, 384 U.S. 757, 771 (1966).

73 Cupp v. Murphy, 412 U.S. 291, 296 (1973).

74 Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 633–34 (1989).

75 Joanne Archambault, *Forensic Exams for the Sexual Assault Suspect*, End Violence Against Women Int'l, 15 (May 2021), https://evawintl.org/resource_library/evawi-training-bulletin-forensic-exams-for-the-sexual-assault-suspect/ [https://perma.cc/48GB-CGZ8]; *see also* U.S. Dep't of Just., Off. For Victims of Crime, *SANE Program Development and Operation Guide, Suspect Examinations*, available at https://www.ovcttac.gov/saneguide/expanding-forensic-nursing-practice/suspect-examinations/ [https://perma.cc/KY8P-PKGQ].

76 *See e.g.*, Del. Code Ann. tit. 14, § 8102A(5) (2023).

77 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

78 *Id.*

79 *Id.* at 2211–12.

80 *Id.* at 2220.

in a specific date/time/location (DTL) range.[81] Geofencing is possible worldwide because companies like Google hoard their users' location data for various purposes.[82]

New technology forces lawmakers and jurists to reconsider approaches to otherwise mundane issues of law and policy. In 1996, Professor Lawrence Lessig offered a revolutionary reading of constitutional protections in *Reading the Constitution in Cyberspace*.[83] Lessig argued that legal constraints "define the domain of security" that individuals have against intrusions, and the legal constraints that govern "real space" also govern cyberspace.[84] Thus, he argues the legal issues in cyberspace can be resolved as if occurring in real space.[85]

Lessig's principle has since been applied to searching cyberspace for a suspect's physical presence with geofences. Some scholars condemn geofences as categorically unconstitutional.[86] Cassandra Zietlow, for example, decried geofences for their "perpetual surveillance."[87] Similarly, Amster & Diehl argue that geofence warrants are unconstitutional due to being exceedingly broad.[88] Even still, geofences were extremely

---

81 Roth, *supra* note 63, at 215.

82 For a more detailed discussion on geofencing specifically, see *id.* And while probably entirely unrelated, I cannot help but laugh at the fact that not long after I published *Drawing Lines*, Google announced it would end its location-data-saving practices that made geofences possible in the first place, making the argument in *Drawing Lines* effectively worthless. *See* Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants that Give Police Access to Location Data*, FORBES (Dec. 14, 2023), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data/?sh=33de6ed92c86 [https://perma.cc/Q87U-558E].

83 Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 899 (1996) ("While regulation in real space is primarily regulation that relies upon the cooperation of the individuals who live under the regulation, regulation in cyberspace can be something different. The code in cyberspace—the software—can enforce its control directly.").

84 *Id.* at 871, 896.

85 *Id.* at 895–96.

86 *See, e.g.*, Cassandra Zietlow, *Reverse Location Search Warrants: Law Enforcement's Transition to 'Big Brother'*, 23 N.C. J.L. & TECH. 669 (2022); Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385 (2022); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2529 ("Simply because the government can obtain location data from private companies does not mean that it should legally be able to.").

87 *See generally* Zietlow, *supra* note 86, at 673 (arguing that reverse location search warrants categorically fall outside the third-party doctrine).

88 *See* Amster & Diehl, *supra* note 86, at 433–34 .

common, and Google received around 180 requests for geofences per week from federal, state, and local law enforcement agencies.[89]

Because geofences rely on user information withheld by Google, they immediately raise concerns about the Fourth Amendment's third-party doctrine. The doctrine states that no unconstitutional intrusion exists when (1) the defendant voluntarily discloses information to a third party and (2) that information is obtained by the police.[90] The doctrine was applied to phone records in *Smith v. Maryland*, where the Supreme Court held that by using his phone, the defendant voluntarily gave his call logs to the telephone company and relinquished any privacy interest in them.[91] The Court broadly held that no one maintained a privacy interest in "business records," defined as information which a consumer typically knows will be (1) conveyed to the company, (2) recorded and retained by the company, and (3) used by the company for legitimate business purposes.[92]

One study shows that a vast majority of consumers know their geolocation data is conveyed and retained by companies, and that it is used for advertising purposes.[93] Accordingly, one might reasonably argue that such data is like the numerical data under *Smith*, and thus "business records" under *Miller*. But in 2018, the Supreme Court declined to extend application of the third-party doctrine to a week's worth of CSLI.[94] The Supreme Court distinguished telephone records in *Smith* from CSLI in *Carpenter* by reasoning that CLSI is not shared "voluntarily" because cell phones became a "pervasive and insistent part of daily life."[95] It held that citizens maintain a legitimate expectation of privacy in their documented physical movements captured by CSLI, thereby invoking the Fourth Amendment.[96]

---

89 Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/D4PT-2PNW].

90 United States v. Miller, 425 U.S. 435, 442, 444 (1976).

91 Smith v. Maryland, 442 U.S. 735, 743–45 (1979).

92 *Id.* at 737, 743–44.

93 BLIS, THE "CURRENCY" OF DATA: QUANTIFYING THE VALUE OF CONSUMER INFORMATION IN 2019, 8 (2019) ("More than ever, people are aware that their data is being collected and used to tailor content and advertising to their interests.").

94 Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

95 *Id.* at 2220 (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)).

96 *Id.* at 2217.

In a separate article, I argue that even post-*Carpenter*, a geofence is not a search within the meaning of the Fourth Amendment when confined to certain temporal limits (i.e., forty-five minutes), because a limited amount of data is subject to the third-party doctrine.[97] This suggestion that *Carpenter* does not bar the third-party doctrine from emerging technologies writ large is strengthened by the Seventh Circuit's recent decision in *United States v. Soybel*, which affirmed that investigators' use of a pen register to identify the perpetrator of a series of cyber-attacks did not constitute a Fourth Amendment search.[98] The Seventh Circuit held:

> IP pen registers are analogous in all material respects to the telephone pen registers that the Supreme Court upheld against a Fourth Amendment challenge in *Smith v. Maryland.* The connection between Soybel's IP address and external IP addresses was routed through a third party—here, an internet-service provider. Soybel has no expectation of privacy in the captured routing information, any more than the numbers he might dial from a landline telephone.[99]

* * *

Three principles of law stem from the above analysis. First, exploitation of advanced technology (e.g., geolocation data, DNA technology, Internet pen registers, etc.) may be reasonable within the meaning of the Fourth Amendment.[100] Second, the revealing characteristics of the fruits of the search are irrelevant when the physical intrusion is minimal.[101] Third, in a warrantless search, the revealing characteristics of the fruits of the search invoke Fourth Amendment protections only when the search reveals an extended account of a person's physical whereabouts and is therefore not a minimal physical intrusion.[102]

---

97 Roth, *supra* note 63.

98 United States v. Soybel, 13 F.4th 584, 594 (7th Cir. 2021), *cert denied*, 142 S. Ct. 835 (2022).

99 *Id.* at 587 (internal citations omitted). The Supreme Court denied Soybel's petition for certiorari, which one might suggest tacitly affirms this analysis. *See* Soybel v. United States, 142 S. Ct. 835 (2022). But of course, "[t]he denial of a writ of certiorari imports no expression of opinion upon the merits of the case[.]" United States v. Carver, 260 U.S. 482, 490 (1923).

100 *See* Smith v. Maryland, 442 U.S. 735, 743–45 (finding the use of a pen register is a reasonable search under the Fourth Amendment); *see also* Soybel, 13 F.4th at 594 (finding the use of IP pen registers is a reasonable search under the Fourth Amendment).

101 *See* Maryland v. King, 569 U.S. 435, 465 (2013).

102 *See* United States v. Jones, 565 U.S. 400, 405–07 (2012); Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

III
CHALLENGING NEUROSEARCHES

A. Evidence

Neuroscientific data has been presented as evidence by both prosecutors and defense attorneys, with early uses in courtrooms dating back to the 1940s.[103] The 1993 decision in *Daubert* formed the current standard for admission of scientific evidence.[104] And the use of exculpatory neuroscientific evidence with the advent of DNA technology satisfies the constitutional protections of due process.[105]

In *Harrington v. State*, the court admitted a brain fingerprinting test, resulting in the exoneration of a man who spent twenty-four years in prison.[106] Dr. Lawrence Farwell conducted this test by measuring Terry Harrington's recognition after being exposed to details of the crime that would be known only to the perpetrator.[107] The test concluded with almost 100% certainty that Harrington did not recognize the information, suggesting that he was not the perpetrator.[108] Dr. Farwell conducted another test that exposed Harrington to visual stimuli of his alibi (a musical concert), that detected a P300 response[109] demonstrating a similar certainty.[110] And in 2010, a court

---

103 Francis X. Shen, *The Overlooked History of Neurolaw*, 85 FORDHAM L. REV. 667 (2016). *See also* Nita A. Farahany, *Neuroscience and Behavioral Genetics in U.S. Criminal Law: An Empirical Analysis*, J.L. AND BIOSCIENCES 485 (2016) (examining judicial opinions between 2005–12 discussing neuroscience or behavioral genetics).

104 Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592–94 (1993). Under the *Daubert* standard, judges may consider the following factors to determine whether scientific methodology is valid and can be properly applied to the facts in issue: (1) whether the theory or technique in question can be and has been tested; (2) whether it has been subjected to peer review and publication; (3) its known or potential error rate; (4) the existence and maintenance of standards controlling its operation; and (5) whether it has attracted widespread acceptance within a relevant scientific community.

105 *See* Paul C. Giannelli, *Ake v. Oklahoma: The Right to Expert Assistance in a Post-*Daubert*, Post-DNA World*, 89 CORNELL L. REV. 1305, 1389 n.546 (2004) (discussing State v. Shuck, 953 S.W.2d 662 (Tenn. 1997), in which "a neuropsychologist's testimony concerning a defendant's acute susceptibility to inducement in support of an entrapment defense was admissible.").

106 Roberts, *supra* note 6, at 264.

107 *Id.*

108 *Id.*

109 The term "P300 response" refers to "a positive event-related potential [brainwave response] that takes place . . . following exposure to a stimulus that is familiar, noteworthy, or useful." *Id.* at 258.

110 *Id.* at 264.

affirmed the use of evidence derived from a quantitative EEG (qEEG) in reducing a death sentence to life in prison.[111] Another court even admitted brain scans to prove a defendant's mental competency.[112] This wide acceptance of neurological data in courtrooms suggests it could easily survive *Daubert* scrutiny. Thus, a defendant challenging neurosearches as inadmissible evidence would likely fail.

B. Constitutionality

Many scholars viscerally reject the compelled search of brain data. Professor Farahany finds that brain data generally encroaches upon one's "sphere of private rumination" or cognitive liberty.[113] Sarah E. Stoller and Paul Root Wolpe find that compelling and using brain imaging and brain fingerprinting may conflict with principles of self-incrimination because the data is coerced, and therefore unreliable testimony, and the use of such data may invade one's privacy.[114] And Matthew Baptiste Holloway argues the same for functional MRIs.[115]

But Kiel Brennan-Marquez offers a separate perspective in *A Modest Defense of Mind Reading*.[116] Brennan-Marquez suggests that scholars who reject the compelled acquisition of brain data (what he calls the fictional "Mind Reader Machine") as a de facto violation of the Fifth Amendment are misguided, and that the appropriate analysis concerns the Fourth Amendment.[117] He ultimately concludes that "certain uses of the Mind Reader Machine would likely be permitted, others would likely be prohibited, and either way, the determination would

---

111 Terry Lenamon & Reba Kennedy, *QEEG Brain Mapping Evidence and Mitigation in South Florida's Grady Nelson Trial*, Death Penalty Blog (Dec. 7, 2010), https://www.deathpenaltyblog.com/qeeg-brain-mapping-evidence-and-mitigation-in-south-floridas-grady-nelson-trial/ [https://perma.cc/BR5L-EQ8Q]; State v. Nelson, No. F05-846, 2010 Fla. Cir. LEXIS 15125 (11th Fla. Cir. Ct. Dec. 3, 2010), *aff'd*, 206 So. 3d 54 (3d Fla. Dist. Ct. App. 2015) (per curiam).

112 Van Middlesworth v. Century Bank & Tr. Co., No. 215512, 2000 WL 33421451, at *2 (Mich. Ct. App. May 5, 2000) (per curiam).

113 *See generally* Farahany, *Incriminating Thoughts*, *supra* note 3, at 406.

114 Sarah E. Stoller & Paul Root Wolpe, *Emerging Neurotechnologies for Lie Detection and the Fifth Amendment*, 33 Am. J.L. & Med. 359, 366 (2007).

115 Matthew Baptiste Holloway, Comment, *One Image, One Thousand Incriminating Words: Images of Brain Activity and the Privilege Against Self-Incrimination*, 27 Temp. J. Sci. Tech. & Env't. L. 141, 174 (2008).

116 Kiel Brennan-Marquez, *A Modest Defense of Mind Reading*, 15 Yale J.L. & Tech. 214 (2013).

117 *Id.* at 257.

be contextual and technology-specific."[118] But like Farahany, Brennan-Marquez proffered this theory before *Carpenter*,[119] geofences,[120] and the commercialization of neurotechnology.[121] A revisit of this analysis is thus warranted.

No court would reasonably hold that a person *does not* have a reasonable expectation of privacy in their private thoughts.[122] The relevant inquiry is whether a neurosearch warrant is (1) supported by probable cause and (2) particular in time, location, and scope to ensure that there is a fair probability that evidence of a crime would be obtained.[123] Alternatively, in considering the third-party doctrine, whether acquisition of commercial brain data is a search at all.[124]

Probable cause is "a fair probability that contraband or evidence of a crime will be found in a particular place."[125] Particularity "safeguard[s] the privacy and security of individuals against arbitrary invasions" by government actors.[126] The particularity of a warrant's scope can be broadly worded because courts find it "unnecessary to distinguish between the things that may be taken from those that must be left undisturbed."[127] But a request to search a whole home for "evidence of crime" would not be particular enough because it does not particularly

---

118 *Id.* at 271.

119 Carpenter v. United States, 138 S. Ct. 2206 (2018) (holding that acquiring seven days' worth of cell-site location information was a search within the Fourth Amendment).

120 Valentino-DeVries, *supra* note 89 (stating federal agents first made geofence requests to Google in 2016, according to Google employees).

121 *See supra* notes 31–35 and accompanying text.

122 *See* Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1879 (2005) ("If one has an expectation of privacy anywhere, it is likely to be in the contents of one's own mind. Moreover, the Court has made clear that it is not necessary that for a search to occur there must be a physical trespass or touching.").

123 In re Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 740–41 (N.D. Ill. 2020) (ruling that a geofence warrant for a forty-five-minute time space was too broad and thus failed the constitutional requirements of particularity).

124 *See infra* note 143 (listing sources documenting acquisition of commercial DNA data).

125 Illinois v. Gates, 462 U.S. 213, 238 (1983).

126 Camara v. Municipal Court of San Francisco, 387 U.S. 523, 528 (1967).

127 United States v. Mason, No. 92-CR-1069, 1993 WL 191806, at *1 (N.D. Ill. June 4, 1993), *aff'd*, 42 F.3d 1392 (7th Cir. 1994) ("The search warrant authorized the agents to search the residence for and seize 'any and all documents and records related in any way to Martha Hoover, Colleen Etheridge, Karen Casey, Marsha Woods, Lynn Townsend, Leroy Gain and Carolynn Anderson.'").

describe the evidence to be acquired.[128] The brain data corollary would be a prohibition on the authorization to search the whole brain for evidence of crime. But as discussed, the contemporary understanding of categorical neuroscientific evidence suggests it would be easy to establish probable cause that the brain data existed and that the type of data sought could be narrowed.[129]

The constitutionality of neurosearches depends heavily on whether the data is recovered directly from the user or from a third party. Investigators could reasonably employ any of the discussed commercial neurotech products in criminal investigations.[130] Like the procedures in a compelled SAFE, police could compel a suspect to submit to an EEG or MRI. Despite the comprehensive revealing properties of brain data, the physical invasion required to extract it is minimal because it only requires placement of a headset on the suspect. Like the "revealing power of [the defendant's] DNA" seized with a cheek swab contemplated in *Maryland v. King*, brain data captured exclusively from placing a headset on a suspect would likely be reasonable under the Fourth Amendment.[131]

But a suspect's brain data recovered from commercial neurotechnology companies is not so clear cut. Until *Carpenter v. United States*,[132] the third-party doctrine permitted warrantless searches of CSLI by allowing investigators to issue an investigative subpoena to telecom companies. But the Supreme Court diverted course and protected the public from the detriment of freely contracting away their data.[133] But I contend that *Carpenter* has been misinterpreted and too broadly applied, especially given the Court specifically stated that *Carpenter* was a "narrow" decision.[134]

Paramount to conceptualizing a challenge to the exploitation of brain data held by third parties is understanding the rationale behind *Carpenter*. Warrantlessly obtained CSLI spooked

---

128 United States v. Sanchez-Jara, 889 F.3d 418, 421 (7th Cir. 2018).

129 *See supra* Part I.A.

130 *See supra* Part I.B.

131 *See supra* note 68 and accompanying text. Memorialized and uttered brain data evidence requires recording a response to stimuli, suggesting a potential violation of the Fifth Amendment. But again, assuming *arguendo* that this evidence is physical as opposed to testimonial, a compulsory search would likely survive constitutional scrutiny due to the minimal physical intrusion.

132 Carpenter v. United States, 138 S. Ct. 2206 (2018).

133 *Id.* at 2217.

134 *Id.* at 2220.

the Justices because of how easy it was to obtain an "exhaustive chronicle" of a defendant's *geographic* whereabouts. But strictly speaking, brain data poses no such threat.[135]

The *Carpenter* Court held that unlike *Smith* and *Miller*, users retained a legitimate expectation of privacy in the record of their "physical movements" through CSLI.[136] In the amicus brief Google submitted in *United States v. Chatrie*,[137] Google itself argues that *Carpenter* should apply to geolocation data in geofence warrants.[138] Google argued that "as in *Carpenter*, the fact that users voluntarily choose to save and share [location history] information with Google does not on its own implicate the third-party doctrine, to the extent that doctrine is still viable."[139] Google argued the Supreme Court's reasoning in *Carpenter* that cell phones and their services are a "pervasive and insistent part of daily life" similarly applied to location-based services.[140] Some courts that have analyzed geofence warrants have agreed with this analysis, in that disabling the multiple location tracking services built into cell phones and applications could be complicated for the user and render the phone or application completely unusable.[141] Lastly, the *Carpenter* Court left open whether CSLI *could* be subject to the third-party doctrine if confined to a certain time limit:

> [W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.[142]

Understanding this, it is difficult to strictly apply *Carpenter* to commercial brain data owned by third parties. First, brain data does not inherently reveal a person's whereabouts. DNA and brain data are perhaps equally revealing, but both are

---

135 *Id.* at 2219, 2223.

136 *Id.* at 2217.

137 590 F. Supp. 3d 901 (E.D. Va. 2019).

138 Brief of Amicus Curiae Google LLC at 20–22, United States v. Chatrie, 590 F. Supp. 3d. 901 (E.D. Va. 2019) (No. 3:19-cr-00130-MHL).

139 *Id.* at 22.

140 *Id.*

141 *See, e.g.*, State v. Muhammad, 451 P.3d 1060, 1072 n.3 (Wash. 2019) ("turning off multiple location tracking services built into our cell phones can be a complicated process, and disabling these services render many apps less usable. Or in some cases, completely unusable.") (internal citations omitted).

142 Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

more revealing than a user's geolocation data. And scholars have documented instances when DNA owned by third parties (23andMe, etc.) has been acquired and exploited in criminal investigations.[143] While location data may be incorporated into commercial neurotech, it's possible for companies to parse out such data before turning it over to investigators (and investigators seeking geolocation data would likely search elsewhere).

Second, unlike the geolocation data, which effectively enables other aspects of the device to function, the exchange of brain data between user and company is explicit, voluntary, and is the *sole purpose of the transaction* (e.g., analytics by the company).[144] So brain data is incomparable to involuntarily shared geolocation data, which drove the Supreme Court to limit the third-party doctrine and is likely afforded protection commensurate with account-identifying data derived from search warrants executed under 18 U.S.C. § 2703.[145]

Lastly, searches for brain data held by third parties are easier to narrow down than tower dumps or geofences.[146] Many geofence warrants are denied as a matter of particularity because many users other than potential suspects are identified in the process. For example, a geofence warrant for a forty-five-minute limit of a Chicago residential building was too broad and thus failed the constitutional requirements of

---

143 *See, e.g.*, Jesse Kitnick, *Killer's Code: Familial DNA Searches Through Third-Party Databases Under* Carpenter, 41 CARDOZO L. REV. 855, 862–63, 869 (2019); Evan Enzer, *Familial DNA Searches Using Public Databases and the Third-Party Doctrine*, BERKELEY TECH. L.J. BLOG (Nov. 6, 2019), https://btlj.org/2019/11/familial-dna-searches-using-public-databases-and-the-third-party-doctrine/ [https://perma.cc/K2LG-XVA5]. *See also* Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823, 857 (2022) ("DNA, the substance that literally makes a person one of 'we the people,' is potentially accessible to government agents under the modern Court's third-party approach.").

144 But again, this voluntariness becomes questionable when employers require employees use it as a condition of employment. *See supra* Part I.B.

145 Law enforcement agencies use the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2703(a), 2703(b), and 2703(c), as the mechanism to compel Google to disclose records and other information particularly described in the geofence warrant. But these statutes permit the seizure of any data associated with the user's account such as name, phone number, email address, etc. And the government can compel social media companies to preserve this information for up to 180 days while law enforcement seeks a warrant. 18 U.S.C. § 2703(f). Despite this statutory requirement, the companies are inherently motivated to retain the data anyway, because it enables them to tailor advertisements to users and sell the data to data-miners. *See* BLIS, THE "CURRENCY" OF DATA: QUANTIFYING THE VALUE OF CONSUMER INFORMATION IN 2019, 13 (2019).

146 *See supra* Part II.C (defining tower dumps and geofences).

particularity.[147] But executing a search warrant on a neurotech company requires investigators to already have a suspect and evidence that the suspect uses that company's product. And unlike the unaffiliated users caught in the Chicago geofence, brain data collected and stored by commercial neurotech companies are segregated by user. Thus, *Carpenter* and its progeny do not prohibit government searches of brain data held by third parties.

Conclusion

This Note presents a modern analysis on the constitutionality of compulsory searches of neuroscientific evidence in criminal investigations. Scholars have condemned its use as a violation of the Fifth Amendment, but seldom analyze it under the Fourth.

The Supreme Court considers the revealing characteristics of DNA irrelevant because the physical intrusion required for its collection — a cheek swab — is minimal. Commercial neurotech is just as noninvasive, resembling headphones or a wristwatch. Thus, searches of a person for proprietary brain data likely survive constitutional muster. And the evolution of the Fourth Amendment's third-party doctrine suggests that extensive geolocation data revealing a "comprehensive dossier" of a user's whereabouts transcends the definition of business records. But commercial brain data is user-specific, and any tangential geolocation data can be parsed before being transferred to investigators. Commercial brain data more resembles the Supreme Court's definition of "business records" than the geolocation data that led to *Carpenter*. Thus, governments can properly acquire the brain data from commercial neurotech companies under the third-party doctrine without probable cause to search a specific user.

Scholars like Professor Nita Farahany have been sounding the alarm for over a decade, practically demanding a codified right to cognitive liberty. This Note serves as support for her position, for it shows that existing constitutional law likely fails to adequately protect the public from neurosearches.

---

147 *See* In re Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020).