GET OUT OF MY HEAD: AN EXAMINATION OF POTENTIAL BRAIN-COMPUTER INTERFACE DATA PRIVACY CONCERNS

KEVIN Y. LI

Abstract: Brain-computer interfaces ("BCI"), which interpret brain impulses and translate them into real world outputs, currently exist in a variety of forms. With the continued development of BCIs and their increasing complexity, privacy issues will arise in regards to the data that they collect. Existing federal statutes, such as HIPAA, as well as state data privacy statutes offer some protection to BCI users, but it remains to be seen whether these laws will be sufficient to accommodate the amount and sensitivity of the data likely to be generated by future BCIs. Lastly, this article explores the possibility of admitting data generated from BCIs as evidence in courtrooms, with consideration given to how much intrusion on mental privacy is constitutionally acceptable.

I. INTRODUCTION

The concept of controlling things in the physical world with the human mind is one that has permeated science fiction novels and movies around the world.¹ However, this popular fantasy is now moving closer to practical reality with the advent of brain-computer interfaces ("BCI"), alternatively known as brain-machine interfaces ("BMI").² Some of these devices are already in use for mainly medical purposes, while many have contemplated a broader range of uses including human enhancement.³ At a general level,

¹ See, e.g., CARRIE (Doubleday 1974); PSYCHOKINESIS (Redpeter Film 2018); X-MEN (Marvel Enterprises 2000).
BCIs consist of receptors that record electric signals sent from the brain and software that translates them into a tangible output in real time.\(^4\)

While the potential for these devices to improve human health and enjoyment is great, there are considerable challenges that come with the development of such technology.\(^5\) One challenge is the concern over the privacy of the data generated from these brain receptors.\(^6\) In addition to nationwide regulation by agencies such as the Federal Trade Commission (“FTC”) and the Food and Drug Administration (“FDA”), states have independently enacted statutes that affect the handling of health related data.\(^7\) BCIs present a further challenge since, unlike other types of wearable medical devices, the data that they collect could essentially allow access into one’s thoughts.\(^8\) Thus, it is important to analyze how these inventions interact with existing privacy laws as well as how policy might shift in the future in order to keep pace with this promising technology.\(^9\)

II. AN OVERVIEW OF BRAIN-COMPUTER INTERFACE TECHNOLOGY

The first predecessor to a BCI was an experiment performed by Dr. Grey Walter in 1964, where he was able to generate an output by placing electrodes directly on the brain of a patient undergoing surgery.\(^10\) Since then, a wide variety of BCIs have been developed and

\(^{4}\) Id. at 201.
\(^{5}\) See id. at 202–03 (acknowledging societal challenges that accompany new technology).
\(^{6}\) Id. at 205.
\(^{7}\) See infra notes 35–39 and accompanying text.
\(^{8}\) Krausová, supra note 3, at 205.
\(^{9}\) See id. (identifying the need for the law to safeguard the privacy of BCI data).
\(^{10}\) Id. at 200.
utilized. Some of these are invasive while others operate as wearable devices. While most BCIs relay signals out to an interface, some also feed information back into the brain. Currently, the most common application for these interfaces are medical devices, although human enhancement is a developing field.

A. Medical Devices

One common use of BCI today is prosthetics. Amputees have been able to achieve significant amounts of control over prosthetics by the use of sensors that detect electrical impulses from the brain and convert them into proportional movements of the replacement limb. There has also been recent innovation in developing technology that would allow prosthetic limbs to feed sensory information back to the brain, further restoring function for affected patients. Other applications include signal-to-output devices which allow patients with conditions such as locked-in syndrome to communicate their thoughts, and the widely recognizable cochlear implant, an example of an interface that sends sensory data unilaterally from the world into the brain.


See id. at 120–21 (describing implants as well as wearable BCIs).

Id. at 128.

See Krausová, supra note 3, at 202 (explaining various BCI applications).

Chan, supra note 11, at 121.

Id. at 122.

Krausová, supra note 3, at 201.

Chan, supra note 11, at 129; Krausová, supra note 3, at 200.
B. Human Enhancement

The ability of BCIs to integrate brain activity with computer algorithms has far-reaching implications in terms of expanding human capability.\(^1\) A striking example of this is an invention by the New York based CTRL-Labs which consists of a wearable arm sleeve that records brain impulses and converts them into movements of a cursor on a screen.\(^2\) While CTRL-Labs has demonstrated using this device to play computer games and type with just brain signals, one of their science advisors has stated that an eventual application of this technology may be to control complex prosthetic or external devices with relative ease.\(^3\) Futurists have also posited ideas such as the eventual emergence of interfaces that can improve human memory and cognitive function by creating an open two-way link between the brain and a computing device.\(^4\)

III. HEALTH DATA PRIVACY REGULATIONS

A. HIPAA

1. An Overview of the Legislation as it Pertains to Wearable Devices

The Health Information Portability and Accountability Act (“HIPAA”) as well as the Health Information Technology for Economic and Clinical Health Act (“HITECH”) are two pieces of federal regulation that may have privacy implications for data collected by

\(^1\) See Levy, supra note 2 (suggesting the development of complex BCIs superior to natural limbs).
\(^2\) Id.
\(^3\) Id.
BCIs. HIPAA authorized the Department of Health and Human Services (“HHS”) to impose regulations that ensure the safety of data that contains protected health information ("PHI"). PHI is information that would identify the person to which the information pertains and is relevant to that individual’s physical or mental health. HIPAA originally applied to only healthcare providers and insurance companies, but HITECH expanded HIPAA’s scope to include business associates—third parties that create, receive, maintain, or transmit PHI for functions such as data analysis, processing, or administration with healthcare providers or insurance companies. Currently, most manufacturers of wearable devices like the Apple Watch are not covered under HIPAA because they do not interact directly with healthcare providers or insurance companies and are thus not within the definition of business associates.

2. Brain-Computer Interfaces and HIPAA

The applicability of HIPAA to developers of BCIs will likely turn on how medically relevant each BCI in question purports to be. BCIs such as limb prosthetics and cochlear implants fall well within the PHI requirement of HIPAA and their manufacturers are also

24 Health Insurance Portability and Accountability Act § 262.
25 Id. § 262.
26 Health Information Technology for Economic and Clinical Health Act § 13401.
28 See Health Information Technology for Economic and Clinical Health Act § 13401 (expanding HIPAA’s scope to include business associates of covered entities); Health Insurance Portability and Accountability Act § 262 (creating requirements for handling of personally identifiable health information by certain healthcare entities); Arnow, supra note 27, at 631–32 (suggesting that HIPAA would cover wearable devices that are considered regulated medical devices).
considered business associates since they would necessarily have to relay data to and from doctors and insurance companies in order to implement their devices.\textsuperscript{29} The more difficult question is evaluating the status of human enhancement BCIs such as the armband that CTRL-Labs is developing, since these BCIs seem to fall into the middle ground between the realm of covered medical device BCIs and the currently uncovered wearable health devices such as the Apple Watch.\textsuperscript{30}

Human enhancement BCIs should have no difficulty falling within the scope of PHI since the concept of BCI is inherently individualized and the brain impulse data recorded by the device can be construed as to be within the definition of relating to mental or physical health.\textsuperscript{31} Developers of human enhancement BCIs, however, may be able to elude HIPAA regulation in the sense that, like manufacturers of wearable devices such as the Apple Watch, they too might not directly transfer their gathered data to healthcare providers or insurance parties.\textsuperscript{32} What may distinguish BCIs from current wearable devices in this

\textsuperscript{29} See Health Information Technology for Economic and Clinical Health Act § 13401 (expanding HIPAA’s scope to include business associates of covered entities); Health Insurance Portability and Accountability Act § 262 (creating requirements for handling of personally identifiable health information by certain healthcare entities); Chan, supra note 11, at 121, 129 (describing the use of BCI in limb prosthetics and cochlear implants).

\textsuperscript{30} See Health Information Technology for Economic and Clinical Health Act § 13401 (expanding HIPAA’s scope to include business associates of covered entities); Health Insurance Portability and Accountability Act § 262 (creating requirements for handling of personally identifiable health information by certain healthcare entities); Arnow, supra note 27, at 628–29 (explaining that data from wearable devices like the Apple Watch are typically not handled by HIPAA and HITECH’s covered entities); Levy, supra note 2 (describing a wearable BCI device for controlling a cursor using neuronal impulses).

\textsuperscript{31} See Health Insurance Portability and Accountability Act § 262 (defining PHI as information that would identify the person and that is relevant to the person’s physical or mental health); Levy, supra note 2 (providing an example of a potentially human enhancing BCI device that records data about the user’s body).

\textsuperscript{32} See Health Information Technology for Economic and Clinical Health Act § 13401 (expanding HIPAA’s scope to include business associates of covered entities); Health
context is that BCIs in the near future may require specialized interactions with healthcare providers in order to be utilized effectively. Unlike something like an Apple Watch which is easily understood and may be used straight from the box, CTRL-Lab’s wearable armband may require additional setup or maintenance which in turn may necessitate consultation with neurologists and insurance companies. Additionally, future users of BCIs may return to their healthcare providers with information generated from their devices in the same way that users of wearable fitness devices are starting to introduce gathered data during doctors’ visits.

B. Expanding State Privacy Regulations

1. Recent State Legislation Regarding Data Privacy

In the wake of an increase in electronically stored information and subsequent data breaches, individual states have enacted policies in order to further protect their residents’ sensitive data. In 2012, Texas enacted the Texas Medical Records Privacy Act, which

_________________________________________________________
Insurance Portability and Accountability Act § 262 (defining covered entities as health plans, clearinghouses, and providers).
33 See Arnow, supra note 27, at 607–08 (describing the ubiquity and usability of current wearable electronic sensor devices); Levy, supra note 2 (giving an example of a technologically complex human enhancement BCI device).
34 See Levy, supra note 2 (describing a lengthy training process for performing new kinds of brain commands using BCI).
35 See Arnow, supra note 27, at 628 (indicating that wearable device consumers have begun to share device data with physicians).
expanded the scope of HIPAA in the state.\textsuperscript{37} The act mandates that, in addition to healthcare providers and insurers, any people or businesses that come into contact with PHI must have training and then authorization from an individual in order to use their information.\textsuperscript{38} Florida bolstered its data breach notification requirements in 2014 with the Florida Information Protection Act.\textsuperscript{39} This act expanded protection of personal information, like names and social security numbers, to include things such as medical history and mental or physical condition.\textsuperscript{40} This act also expanded covered parties from just entities that conducted business in the state to include any entity that acquires, stores, or uses such information in the state.\textsuperscript{41} In 2015, California amended its statute to require any businesses that maintain personal information of residents to employ reasonable security measures in order to protect their information.\textsuperscript{42}

2. Brain-Computer Interfaces and State Privacy Regulations

State-enacted regulations can improve the security of personal data generated from current and future BCIs either through broadening of existing policies or through creation of new incentives.\textsuperscript{43} The Texas, Florida, and California statutes all expanded the coverage of data security regulations, which is an important trend for eventual consumers of BCI.\textsuperscript{44} As companies begin to develop BCI for the purpose of large scale entertainment and

\textsuperscript{37} \textit{Tex. Health & Safety Code Ann.} § 181.001(b)(2).
\textsuperscript{38} \textit{Id.} § 181.001(b)(2), 181.101, 181.154.
\textsuperscript{39} \textit{Fla. Stat.} § 501.171.
\textsuperscript{40} \textit{Id.} § 501.171(1)(g)(1).
\textsuperscript{41} \textit{Id.} § 501.171(1)(b).
\textsuperscript{42} \textit{Cal. Civ. Code} § 1798.81.5(b).
enhancement, there will likely be an increase in data flow generated.\textsuperscript{45} A data breach that exposes PHI from BCI would be particularly disastrous since thoughts, impulses, and emotional data may be exposed on a massive scale.\textsuperscript{46} Thus, states have every incentive to continue in the direction of laws that encourage vigilant protection of their consumers’ PHI, such as in the amended California regulation, and that impose stricter regulations on reporting suspected breaches, such as in the Florida Information Protection Act.\textsuperscript{47}

IV. A CONSTITUTIONAL CHALLENGE TO BCI DATA AS EVIDENCE

\textit{A. The Fifth Amendment and Wearable Device Data}

Corporations and fellow consumers are not the only parties that BCI users might worry about in regards to who might access their private information.\textsuperscript{48} An anxiety long held by private citizens in the digital age is that their personal data might be used against them by the government.\textsuperscript{49} In July 2017, an Ohio state court held that medical data gathered from a defendant’s pacemaker was admissible evidence in determining whether or not he committed arson.\textsuperscript{50} A cardiologist testified that the readings from the instrument were


\textsuperscript{46} See Krausová, supra note 3, at 205 (describing the potential ability of BCIs to record emotional and mental data); Baker, supra note 36 (reporting a data breach at a major entertainment and gaming corporation).

\textsuperscript{47} See CAL. CIV. CODE § 1798.81.5(b); FLA. STAT. § 501.171; TEX. HEALTH & SAFETY CODE ANN. § 181.001.


\textsuperscript{49} See id. (noting that the increasing reliance on personal data has the potential to threaten civil liberties and privacy).

inconsistent with the defendant’s story, which involved rushing many heavy items out of his house through his bedroom window. The court’s decision to admit the evidence is supported by Fisher v. United States, where, in 1976, the Supreme Court held that the Fifth Amendment protection against self-incrimination applies only to testimony and not as a general right of privacy. Such rulings do not help allay concerns of government privacy intrusion, including those of the defendant’s lawyer in the pacemaker case who argued “what is next on this slippery slope as technology advances?”

B. BCI Data as Evidence

The fears expressed by the defendant’s lawyer may begin to be substantiated with the development of BCIs. The judge in that case defended his decision to admit the pacemaker evidence by saying that there was information about things in his body he would be more concerned about than how his heart was beating. These “things in his body” could include the brain signals that give rise to his thoughts, motions, and mental states.

The data collected from BCIs such as CTRL-Lab’s armband may be treated similarly to a pacemaker in terms of admissibility in court since they both represent mostly physical phenomena within one’s body. However, BCIs that collect data directly from the brain

---

51 Id.
53 Judge Rules Pacemaker Data Admissible in Court, supra note 50.
54 See Krausová, supra note 3, at 205 (describing the ability of BCI data to potentially reveal information about mental states); Judge Rules Pacemaker Data Admissible in Court, supra note 50 (warning against government overreach of medical data as technology advances).
55 Judge Rules Pacemaker Data Admissible in Court, supra note 50.
56 See id.
57 See Judge Rules Pacemaker Data Admissible in Court, supra note 50 (summarizing a case where data from a pacemaker was ruled admissible in court); Levy, supra note 2 (explaining that the BCI works by interpreting data sent from the brain).
also can produce information with a mental or emotional component.\textsuperscript{58} For example, a BCI that records brain activity from the amygdala, one of the brain’s emotional regulatory centers, may capture information about the user’s state of mind at different time points.\textsuperscript{59} If a court were to rule this evidence admissible, there could be significant implications, especially since one of the challenges in both criminal and tort cases is ascertaining the subjective mindset of the parties.\textsuperscript{60} While BCI might certainly help establish a party’s mindset, it remains to be seen how accurately future devices will record brain activity and how precisely these electrical stimulations correlate with emotional or mental states.\textsuperscript{61} Even if devices reach a high degree of accuracy in the future, the question for courts to decide is how much personal privacy of thought should be sacrificed for the sake of judicial precision, lest our peace of mind falls down the slippery slope that the lawyer in the pacemaker case cautioned against.\textsuperscript{62}

V. CONCLUSION

While BCI is an exciting and rapidly blossoming field of the present and future, many privacy questions regarding the technology need to be addressed. Although many

\textsuperscript{58} Krausová, supra note 3, at 205.


\textsuperscript{60} See Elizabeth Bennett, Neuroscience and Criminal Law: Have We Been Getting it Wrong for Centuries and Where Do We Go from Here?, 85 FORDHAM L. REV. 437, 445 (2016) (exploring the possibility that neuroscience may reveal information relevant to a party’s mens rea).

\textsuperscript{61} See Krausová, supra note 3, at 205 (explaining that a future aim of BCI technology may be to read minds and identify thoughts).

\textsuperscript{62} See Judge Rules Pacemaker Data Admissible in Court, supra note 50 (reporting the defendant’s lawyer’s remarks about the privacy concerns that accompany developing technology).
BCIs fall within the scope of HIPAA and as a result may be subject to FDA oversight, others may elude federal regulation depending on the nature of the device. States have been responsive to the ever-growing need of increased data protection and enacted legislation appropriately. Many of these statutes would demand greater vigilance over BCI data, although it remains to be seen whether expansion of current protections is sufficient or whether novel legislation is needed to adequately address the enormous privacy risks that these devices generate. Lastly, as neuroscience gives us an increasingly clearer understanding of how mental states correspond to recordable physical data, courts will have to decide just how much of this data should be allowed to be brought before the government or the public in legal matters. Awareness and discussion of these issues will help ensure that this technology allows us to fulfill our fantasy of controlling the world with our minds, instead of allowing others in the world to control what is in our minds.