REGULATING THE SIXTH SENSE: THE GROWING NEED FOR FORWARD-LOOKING DATA PRIVACY AND DEVICE SECURITY POLICY AS ILLUSTRATED BY BRAIN-COMPUTER INTERFACES

Hannah Gallagher*

INTRODUCTION

Although it may not be top-of-mind, many consumers have begun to suspect that technology companies may know a little too much about them for comfort. Journalist, Dylan Curran, decided to investigate and found that Google alone had compiled 5.5 GB[1] (approximately 3 million Word documents) worth of data containing much more invasive information than just his search history. Tech companies use artificial intelligence (AI) to scan users' private emails and continue tracking users' locations even after location settings have been turned off.[2] Companies like Comcast might even soon be able to monitor customers' movement patterns in their homes using Wi-Fi wave signals.[3] Big data is rife with examples of information that could be compromised or abused for surveillance purposes, and the data

* J.D. (2021), Washington University School of Law.

1. "This link includes your bookmarks, emails, contacts, your Google Drive files, all of the above information, your YouTube videos, the photos you've taken on your phone, the businesses you've bought from, the products you've bought through Google . . . They also have data from your calendar, your Google hangout sessions, your location history, the music you listen to, the Google books you've purchased, the Google groups you're in, the websites you've created, the phones you've owned, the pages you've shared, how many steps you walk in a day" Dylan Curran, *Are you ready? This is all the data Facebook and Google have on you,* THE GUARDIAN, (Mar. 30, 2018), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy [https://perma.cc/BQJ2-UQ2G].

2. Dale Smith, *Google collects a frightening amount of data about you. You can find and delete it now,* CNET (June 28, 2020, 7:18 AM), https://www.cnet.com/how-to/what-google-knows-about-you-may-be-a-shock-heres-how-to-download-and-manage-or-delete-your-activity/ [https://perma.cc/F9YT-XT37].

3. They may also be able to read your lips and identify your visitors simply by assessing how Wi-Fi waves bounce off bodies and other objects in houses. Jennifer Miller, *Big Data Probably Knows More About You Than Your Friends Do*, LEAPSMAG (Feb. 5, 2018), https://leapsmag.com/big-data-probably-knows-friends/ [https://perma.cc/4GPS-WJLL]. In one study, MIT researchers used routers and sensors to monitor breathing and heart rates with 99% accuracy. *Id*.

being collected is only becoming more invasive as technology progresses.[4] Devices like smartphones have been tracking users' daily activities for years, but recent advances in health technology are illustrating just how personal the data can become.[5] Wearable fitness trackers, iPhone's Health application, and direct-to-consumer genetic testing companies are just a few examples. Developments like these have drawn their fair share of scrutiny regarding privacy and device security,[6] and while these concerns continue unresolved, even more invasive technology is under development. An example of this is brain-computer interfaces ("BCI"), a biotechnology theoretically capable of augmenting the human brain.[7]

The recent success of Marvel movies such as *Avengers: Endgame* is a testament to society's infatuation with superheroes, but their heightened abilities have always been firmly grounded in science fiction, or so we thought.[8] Modern science and technology, however, are quickly bringing these superhumans much closer to being reality. BCIs, which currently allow users to use neural signals to control external device—such as prostheses, video games, and word processors—have the potential to be used as an elective form of augmenting human brain power.[9] Aside from the scientific advances necessary to usher in this era of augmentative BCI

4. *See, e.g.*, Kim Lyons, *Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments*, THE VERGE (Jan. 31, 2021, 11:26 AM), https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras ("Privacy advocates have raised concerns about how Ring data is used by and made available to law enforcement."); Dan Swinhoe, *The 15 biggest data breaches of the 21st century*, CSO (Jan. 8, 2021, 2:00 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/3HXX-CUYY].

5. *See generally* Curran, *supra* note 1 (Google and Facebook can access location data from multiples devices, user webcams and microphones, and deleted files and search terms).

6. *See infra* Part II.

7. *See* Jerry J. Shih, Dean J. Krusienski & Jonathan R. Wolpaw, *Brain-Computer Interfaces in Medicine*, 87 MAYO CLIN PROC 268–79 (2012).

8. THE WALT DISNEY COMPANY, *Marvel Studios' 'Avengers Endgame' Makes History with $1.2 Billion Global Debut*, THE WALT DISNEY CO. (Apr. 28, 2019), https://www.thewaltdisneycompany.com/marvel-studios-avengers-endgame-makes-history-with-1-2-billion-global-debut/ [https://perma.cc/4BG7-YVNF] ("Marvel Studios' *Avengers: Endgame* has shattered records with an unprecedented estimated global debut of $1.209 billion, becoming the first film in history to surpass $1 billion in its opening weekend.").

9. *See* Daniel Gomez Ramos, *The Future of Brain Computer Interface Technology*, IN-TRAINING (Jan. 22, 2018), https://in-training.org/future-brain-computer-interface-technology-15655 [https://perma.cc/R27R-Y7ZU] for an alternate definition ("BCI is defined as computer technology that can interact with neural structures by decoding and translating information from thoughts (i.e., neuronal activity) into actions.").

usage,[10] the question remains of how to properly regulate the privacy and safety concerns accompanying these devices. Additionally, there are concerns as to the ethical questions surrounding elective alterations of otherwise healthy human minds and bodies.[11] Although not yet a subject of popularized debate, the ways in which society chooses to address policy surrounding BCI could have profound impacts upon the future of humanity.[12] As one scholar emphasized in comparing BCI to genetic enhancements:

> [T]he potential of this technology to change and significantly affect humans is potentially far greater than that of genetic enhancements, because genetic enhancements are inherently limited by biology and the single location of an individual, whereas hybrids of human and machine are not so restricted.[13]

Due to the potential for such transformative impact, it is crucial that policymakers carefully consider the regulations necessary to address the significant privacy and security risks associated with this emerging biotechnology and balance those risks with the interest society may have in encouraging innovation in the sector.

As early as 1998, Kevin Warwick, an Emeritus Professor at Coventry and Reading Universities, was experimenting with adding a little "something extra" to his natural, biological senses.[14] In 2002, he had a 100-electrode micro-array implanted into his wrist and connected to a radio transmitter on his arm.[15] He then used an ultrasonic sensor that

10. For an in-depth analysis of some of the challenges facing researchers, see Eric Chan, *The Food and Drug Administration and the Future of the Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement*, 25 J. MARSHALL J. COMPUT. & INFO. L. 117 (2007).

11. *See, e.g.*, Mark A. Attiah & Martha J. Farah, *Minds, motherboards, and money: futurism and realism in the neuroethics of BCI technologies*, 8 FRONT. SYST. NEUROSCI. 86 (May 15, 2014), https://www.frontiersin.org/articles/10.3389/fnsys.2014.00086/full [https://perma.cc/VST9-2JRV].

12. Kevin Warwick, *Cyborg morals, cyborg values, cyborg ethics*, 5 ETHICS AND INFO. TECH. 131–37 (2003) (discussing possible hazards such as remote controlling the motions of another individual).

13. Ellen M. McGee & Gerald Q. Maguire, *Becoming borg to become immortal: regulating brain implant technologies*, 16 CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS : CQ : THE INT'L J. OF HEALTHCARE ETHICS COMMS. 291–302 (2007).

14. Warwick, *supra* note 12, at 135.

15. Kevin Warwick, *Project Cyborg 2.0*, (Oct. 17, 2019),

communicated with the implant to navigate a room blindfolded using pulses of current to the nerves in his wrist when he was close to an obstacle.[16] This relatively simple experiment illustrated the potential that neuroelectric interfaces (a more rudimentary version of modern brain-computer interfaces) could offer in augmenting human senses.[17]

Since then, scientists have continued to develop applications of the technology for rehabilitative use, and many entrepreneurs have already begun to envision a world where BCIs are used electively to enhance consumers' biology. The recent documentary *I Am Human* explores several themes surrounding these developments.[18] A Wired article about the documentary laid out the possibilities: the ability to see in the dark, a cure for depression, direct mind-to-mind communication, and more.[19]

Not only are these possibilities exciting to think about in the abstract, they are already being implemented by entrepreneurs like Elon Musk and Mark Zuckerberg.[20] Neuralink[21], founded by serial entrepreneur Elon Musk, hopes to eventually be able to offer consumers a host of novel abilities including "being able to access and absorb knowledge instantly from the cloud or to pump images from one person's retina straight into the visual cortex of another; creating entirely new sensory abilities, from infrared eyesight to high-frequency hearing; and ultimately, melding together human and artificial intelligence."[22] Musk has spoken about BCI as a tool to help

---

http://www.kevinwarwick.com/project-cyborg-2-0/ [https://perma.cc/KB2F-BCGA].

16. Eben Harrell, *My Body, My Laboratory,* TIME (Mar. 6, 2011), http://content.time.com/time/magazine/article/0,9171,2050030,00.html [https://perma.cc/QF3M-J7V3].

17. Professor Warwick talks about this experiment on his website. Warwick, *supra* note 15. Interestingly, it is noted that, ". . . Professor Warwick was able to control an electric wheelchair and an intelligent artificial hand, developed by Dr Peter Kyberd, using the neural interface. *Id*. In addition to being able to measure the nerve signals transmitted along the nerve fibers in Professor Warwick's left arm, the implant was also able to create artificial sensation by stimulating via individual electrodes within the array." *Id*.

18. I AM HUMAN (Intelligent Films 2019).

19. *See* Aerielle Pardes, *Brain-Machine Interfaces Could Give Us All Superpowers,* WIRED (May 2, 2019), https://www.wired.com/story/i-am-human-brain-implants/ [https://perma.cc/2MRM-77SW].

20. "Those aren't science-fiction scenarios either. Elon Musk and Mark Zuckerberg have each invested in brain-computer interfaces to advance human capabilities. Musk's Neuralink aims to improve human cognition, to compete with the likes of AI. Zuckerberg's idea is more like a mind-reading machine. Johnson's startup, Kernel, is working on creating a brain interface that develops real world applications of high resolution brain activity." *Id.*

21. *See* NEURALINK, https://neuralink.com/ [https://perma.cc/5MRK-BS6V].

22. *See How Brains and Machines Can Be Made to Work Together,* THE ECONOMIST (Jan. 4, 2018), https://www.economist.com/technology-quarterly/2018/01/04/how-brains-and-machines-can-

balance out the risks posed by highly developed AI technology, which he believes will eventually outpace human intelligence and ability.[23] Furthermore, outspoken entrepreneur Bryan Johnson of Kernel sees BCIs as an inevitable step in the evolution of humanity in the digital age:[24]

> Humans currently reign supreme on planet Earth, because we are the most powerful form of intelligence. . . . We are currently developing a new form of intelligence in the form of AI that is increasingly capable, whether it's conscious or not. For humans to be relevant in a matter of decades there is no choice other than to unlock our brains and intervene in our cognitive evolution. [25]

Although the ideas expressed by these entrepreneurs may sound extreme or even unhinged to some, there is no denying that they are drawing investments, undergoing research and development in labs, and being positioned as a shaping force in society's future.

This is typically how emerging technology works. Policy makers often lag behind, seemingly chasing after the technology and attempting to course correct after the risks to consumers have already manifested themselves.[26] Because of the particularly invasive nature of this technology and its profound risk to data privacy and security, it is crucial to develop a comprehensive policy framework capable of providing adequate consumer protections in the context of highly invasive technology before consumers begin adopting it. With that being said, these risks must also be balanced

---

be-made-to-work-together [https://perma.cc/H2EG-K4HC] [hereinafter *Brains and Machines*]. *See also* Tim Urban, *Neuralink and the Brain's Magical Future*, WAIT BUT WHY (Apr. 20, 2017), https://waitbutwhy.com/2017/04/neuralink.html#part6 [https://perma.cc/V2FL-7F2X].

23. *See* Urban, *supra* note 22.

24. Johnson is developing what is described as "a non-invasive mind/body/machine interface (MBMI) to improve, evolve and extend human cognition" at his company Kernel. *See* KERNEL, https://kernel.com/ [https://perma.cc/L5SC-CUDN].

25. Steven Levy, *Why You Will One Day Have a Chip in your Brain*, WIRED (July 5, 2017), https://www.wired.com/story/why-you-will-one-day-have-a-chip-in-your-brain/ [https://perma.cc/C92W-N2N8].

26. Some modern examples of this include Juul and 23andMe data sales. *See* Ainsley Harris, *How Juul, founded on a life-saving mission, became the most embattled startup of 2018*, FAST COMPANY (Nov. 19, 2018), https://www.fastcompany.com/90262821/how-juul-founded-on-a-life-saving-mission-became-the-most-embattled-startup-of-2018 [https://perma.cc/VU94-RPYD]. *See also* Henri-Corto Stoeklé et al., *23andMe: a new two-sided data-banking market model*, BMC MEDICAL ETHICS 17 (2016) at 1, 11.

with the technology's potential to enhance the human condition and improve users' lives. Although it can be difficult to fully analyze the potential impact of an emerging technology with yet to be realized potential, it is important to begin evaluating relevant policy frameworks as soon as possible in order to minimize what is seemingly an inevitable lag between technology and the law.[27]

Part I of this Note will outline the current state of augmentative BCI technology, from its origin as a rehabilitative tool developed in medical research labs through its journey to market in modern biotech start-ups. Part II will discuss the trend of increasingly invasive technology, of which BCI is merely one example, and highly personalized data being collected by companies. It will also outline current developments in data privacy and device security regulation. Finally, Part III will examine proposed policy solutions for governing data privacy and device security in a manner that will tackle the challenges of BCI and other invasive consumer technologies.

I. BCI RESEARCH AND DEVELOPMENT

Practical applications of BCI technology are often seen in clinical settings, seeking to rehabilitate or mitigate the effects of damage to the central nervous system.[28] Research universities and other neuroscience entities have been working on this technology for decades, slowly making progress towards a better understanding of neural signals and how to leverage them in combination with computer interfaces.[29] Advances in BCI have been unpredictable and relatively slow (in comparison with the rate of progression in other spheres of technology[30]) due to several developmental barriers.[31] Like early computers, current BCI has some serious bandwidth

27. Robin Tricoles, *Smart tech sprints forward, but the law lags behind*, ARIZ. STATE UNIV. (Mar. 21, 2019), https://research.asu.edu/smart-tech-sprints-forward-law-lags-behind [https://perma.cc/QY9Y-VK6X] (referencing pacing problem caused by existing laws inability to keep up with rapidly developing new technologies).

28. *See, e.g.*, Shih et. al., *supra* note 7.

29. *See, e.g.*, Ed Boyden, MIT MCGOVERN INST., https://mcgovern.mit.edu/profile/ed-boyden/ [https://perma.cc/ZB87-NXBX] (last visited May 24, 2021); Brain Computer Interface, CARNEGIE MELLON UNIV.: BIOMEDICAL FUNCTIONAL IMAGING AND MICROENGINEERING LAB, https://www.cmu.edu/bme/helab/Research/BCI/index.html [https://perma.cc/DM3L-TPTR] (last visited May 24, 2021).

30. Urban, *supra* note 22, at 97–98.

31. *Brains and Machines*, *supra* note 22.

limitations because there have never been more than a "couple hundred electrodes in the human brain" limiting the number of neurons that can simultaneously be recorded.[32] It is estimated that the number of neurons that can be recorded doubles every 7.4 years.[33] This stands in stark contrast to computers, where the number of transistors that can fit onto a computer chip, increasing computing power, doubles about every 18 months.[34] Additionally, there are problems of implantation methods, biocompatibility, and device lifespan.[35] Finally, there is significant potential for financial and organizational barriers to progress. [36] Thus, the inherently complex nature of the technology is one barrier to rapid progress.

Despite these challenges, when the industry started to draw big names like Elon Musk and Facebook, venture capital investments were not far behind. For example, in 2016, entrepreneur and Braintree founder, Bryan Johnson, invested $100 Million into Kernel to "read and write neural code."[37] This influx of capital into the market will certainly help eliminate some of the barriers to development. In fact, despite the thresholds that remain to be crossed in BCI development, the projected Compound Annual Growth Rate (CAGR) for the global BCI market over the next 5 years ranges from 12.43% to 14.9%.[38] Estimates for market size globally range from $283.04 million to up to $1.2 billion by 2025.[39] Due to the nature of technological advancement and adoption, it is useful to conceptualize BCI applications in the near-term—namely rehabilitating patients, piloting non-

32. "When it comes to vision, that equals a super low-res image. When it comes to motor, that limits the possibilities to simple commands with little control. When it comes to your thoughts, a few hundred electrodes won't be enough to communicate more than the simplest spelled-out message." Urban, *supra* note 22 at 97–98.

33. Urban, *supra* note 22.

34. Urban, *supra* note 22.

35. Urban, *supra* note 22.

36. *Brains and Machines*, *supra* note 22 ("One is financial: the combination of lengthy payback periods and deep technology scares off most investors. Another is the need for multidisciplinary expertise to get better interfaces built and management skills to keep complex projects on track.").

37. *Brains and Machines*, *supra* note 22.

38. *Global brain computer interface market size 2018 and 2025*, STATISTA, https://www.statista.com/statistics/1015013/worldwide-brain-computer-interface-market-value/ [https://perma.cc/J7QA-B4AH] (last visited Feb. 5, 2020); *Brain Computer Interface Market to be Worth US$ 1.2 Billion by 2024; Demand Increases with Growing Prevalence of Brain Disorders,* TRANSPARENCY MKT. RSCH (May 16, 2018, 4:30 AM), https://www.prnewswire.com/news-releases/brain-computer-interface-market-to-be-worth-us-12-billion-by-2024-demand-increases-with-growing-prevalence-of-brain-disorders---tmr-682767451.html [https://perma.cc/HA9Y-EE66].

39. TRANSPARENCY MKT. RSCH., *supra* note 38.

invasive consumer devices, and beginning human tests with more invasive devices—than applications in the long-term. As the technology evolves from clinical use to augmentative use, though, several considerations—such as more widespread use, parallel developments in AI, and more rapid scientific advancement due to funding increases—will make a more comprehensive privacy and security policy necessary to encourage the safety of the emerging technology while minimizing risks.

A. Near-Term Implementation of BCI

Scientists have already seen a degree of success in implementing various BCI (and BCI adjacent technologies) in individuals whose central nervous system has been compromised to the extent that their standard neural signals are no longer functioning to control certain movements.[40] At Brown University, a quadriplegic hardwired to a computer with BrainGate[41] was able to beat a reporter at a video game using a cursor being controlled entirely with neural signals.[42] At Emory University, a survivor of a brain stem stroke[43] is now able to use brain signals to spell out words and select phrases as a means of communication.[44] Additionally, BCI has the potential to greatly improve the lives of patients using prosthetic limbs. Traditionally, using a prosthetic limb "requires training, extra effort and can have a certain amount of awkwardness to it."[45] However, the hope is that using BCI a patient can use neural signals–already associated with muscle movement in

40. Morgan B. Lee et al., *Brain-Computer Interfaces in Quadriplegic Patients*, 30 NEUROSURG CLIN N AM 275–81 (2019).

41. BrainGate is a company specializing in rehabilitative applications of BCI. The company's about page explains, "Our research team includes leading neurologists, neuroscientists, engineers, computer scientists, neurosurgeons, mathematicians, and other researchers – all focused on developing brain-computer interface (BCI) technologies to restore the communication, mobility, and independence of people with neurologic disease, injury, or limb loss." *See* BRAINGATE, https://www.braingate.org/about-braingate/ [https://perma.cc/QD2C-FMZB].

42. Paul R. Wolpe, *Ethical and Social Challenges of Brain-Computer Interfaces*, 9 AM. MED. ASS'N J. ETHICS 128, 128 (2007).

43. The patient J.R. suffers from locked-in syndrome after his stroke. *See id.* "The locked-in syndrome (pseudocoma) describes patients who are awake and conscious but selectively deefferented, i.e., have no means of producing speech, limb or facial movements." See https://www.ncbi.nlm.nih.gov/pubmed/16186044 [https://perma.cc/K7UL-MJMC].

44. Wolpe, *supra* note 42.

45. Association of Academic Physiatrists, *Controlling a prosthesis with your brain,* SCIENCEDAILY (Feb. 6, 2017), https://www.sciencedaily.com/releases/2017/02/170206084904.htm [https://perma.cc/Y3J3-JKYB] (last visited Nov 13, 2019).

a healthy limb—to easily control their prosthetic limb.[46] This would give patients hands-free control of the prosthesis, a more natural and manageable experience.[47] In order to demonstrate the full array BCI's application to patient treatment, a 2018 presentation outlined the following possibilities: enabling quadriplegics to use BCI prosthetics, improving stroke patients' motor function, providing "task-related sensations" to amputees, and restoring vision. [48] Clearly, these and other clinical, rehabilitative applications of BCI can serve to improve quality of life and care outcomes for patients with little other recourse.

B. Commercial BCI Development

Many entrepreneurs have begun to envision the potential that this technology holds for electively enhancing human brains. Whether they rationalize this as a means of keeping pace with AI or as a natural continuation of our evolution as a species, the reality is that the commercialization of these technologies as augmentative tools is very possible based upon existing market conditions.[49] Initially, much of the aforementioned estimated market in 2025 is projected to be comprised of non-invasive BCI.[50] This is unsurprising. Currently, non-invasive BCI devices are the only ones that are technologically viable. Further, they are more likely to gain initial market traction since they are less invasive and less permanent, making consumer comfortability more likely.[51] The more invasive BCIs, however, if implemented, will have access to an unprecedented level of personally sensitive information—necessitating

46. *Id.*

47. *Id.* Based upon the described study, researchers say that this technology is in early development but promised to grow rapidly. "The participant learned to activate the knee-unlocking switch on his prosthesis that turned on a motor and unlocked his prosthetic knee. He then proceeded to walk up and down parallel bars while demonstrating his ability to unlock the knee to swing his leg and to sit down. Throughout the study, the participant was able to successfully unlock his knee anywhere from 50 to 100 percent of the time, and he noted (through a questionnaire) his reactions to using BCI with his prosthesis." *Id*.

48. Soc'y for Neuroscience, *Brain-computer interface advances improve prosthetics, therapies: Advances offer help for quadriplegic, stroke, amputee, and blind patients*, SCIENCEDAILY (Nov. 6, 2018), https://www.sciencedaily.com/releases/2018/11/181106121415.htm [https://perma.cc/L2RG-LX6K].

49. *Brains and Machines*, *supra* note 22.

50. TRANSPARENCY MKT. RSCH., *supra* note 38.

51. Urban, s*upra* note 22.

adequate privacy and security protections for consumers.

II. DEVELOPMENTS IN DATA PRIVACY AND SECURITY

Although technology is only now approaching neuro-implantation, privacy and security have been of increasing concern for decades in response to a variety of technological developments. As early as 1890, Justice Louis D. Brandeis wrote about the law's respect for individual privacy—at a time when he was primarily concerned with photography and perceived invasions by the press:[52] "If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression."[53] Much later, the advent of computers and the data that they process has sparked a modern conversation around data privacy. Justices Warren and Brandeis' right to privacy of "thoughts, emotions, and sensations" remains relevant today, especially in light of the potential for augmentative BCI (and the neural data it would no doubt collect).

---

52. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 16–17 (2015).

53. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 206 (1890). The Supreme Court has found the right to privacy to have a constitutional basis. *See* Griswold v. Connecticut, 381 U.S. 479 (1965) (finding zones of privacy to be implied by the "penumbra" of several explicitly guaranteed rights in the Bill of Rights).

A. Non-Federal Developments

1. Data Privacy

The types of neural data that BCIs will collect highlight the significance of privacy protections. Currently, despite the growing national concern over privacy and security relating to technology companies,[54] there is no federal law governing privacy standards. This poses a challenge to implementing a clear standard of privacy protection. While there is no current national framework for data privacy regulation, the California Consumer Privacy Act (CCPA), the EU General Data Protection Regulation (GDPR), and other health data regulation provide relevant examples from which to draw. The CCPA provides, in part, that:

> (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.
>
> (b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.[55]

While the CCPA is regarded as the most comprehensive data law currently enacted in the United States, the GDPR remains the "gold standard," offering the most comprehensive and all-encompassing data protection requirements.[56] The CCPA differs from the GDPR in several ways, such as

54. Kate Fazzini, *In a decade of cybersecurity alarms, these are the breaches that actually mattered*, CNBC (Dec. 23, 2019, 12:01 PM), https://www.cnbc.com/2019/12/23/stuxnet-target-equifax-worst-breaches-of-2010s.html [https://perma.cc/N3RN-FM9M].

55. CAL. CIV. CODE § 1798.100 (West 2019).

56. DataGuidance, *Comparing privacy laws: GDPR v. CCPA*, FUTURE OF PRIVACY FORUM, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [https://perma.cc/5Q8Q-YFBC].

the extent of its collection limitations and its accountability rules. [57] Furthermore, the CCPA excludes medical data from its scope, deferring to federal health data laws, such as the Health Insurance Portability and Accountability Act (HIPAA).[58] Unfortunately, HIPAA was enacted prior to the development of much of today's consumer healthcare technology companies–leaving gaps in the regulatory framework. Concerningly, "Federal and state laws designed to protect [personal health information], such as HIPAA, are only enforced on 'covered entities'—health care providers, health care plans, and research institutions."[59] These laws are not typically enforced on the Internet, and many private companies can solicit health data from users without having to conform to HIPAA regulations."[60] Mobile devices and health applications are a prime example of technology companies operating "outside the purview of HIPAA's protections," since they are not covered entities.[61]

As such, existing privacy legislation tends to leave some ambiguity in regard to health data collected by consumer health technology companies through smartphone applications, wearable devices, and other non-clinical devices. This data, which may fall outside the purview of HIPAA, can turn out to be highly sensitive but lacking adequate protections. This also highlights the fact that sector-specific protections may be too tailored to anticipate future evolutions of the sector, leaving data vulnerable to hybrid markets, like non-clinical smartphone applications.

---

57. *Id.* at 5.

58. § 1798.100, *supra* note 55.

59. *See Concerns Raised About the Sharing of Health Data with Non-HIPAA Covered Entities via Apps and Consumer Devices*, HIPAA J. (Mar. 27, 2019), https://www.hipaajournal.com/concern-sharing-health-data-non-hipaa-covered-entities/ [https://perma.cc/UE9H-85DE].

60. "HIPAA was updated by the HITECH Act of 2009, which does cover electronic medical records and health IT, but does not extend to apps and consumer devices. GDPR covers consumer data collected by apps and consumer devices, but only for companies doing business with EU residents." *Id.*

61. David M. Parker et al., *Privacy and Informed Consent for Research in the Age of Big Data*, 123 PENN ST. L. REV. 703, 710–11 (2019).

2. Device Security Requirements

Furthermore, there are security issues inherent in an emerging technology, such as BCI, that interfaces directly with individuals' neural signals. Not only are the potential implications of cybersecurity failures quite serious in this context,[62] but substantial security standards would seem justified because "brain data may soon give insight into what a particular user may be thinking or what a particular user might be experiencing." [63] These devices would collect, transmit, and possibly store the data in question, making device security vulnerabilities a very real threat to sensitive user data. However, there is a similar lack of federal legislation governing security requirements for hardware devices despite this increasingly apparent need for regulation.

Connected hardware devices—from existing smart home devices to future BCI devices are known to be susceptible to security threats.[64] This is in part because companies focus on making a high volume of smart, connected devices as cheaply as possible. Consumers want smart, interconnected devices that they can afford, and security may be perceived as not worth the expense of developing. However, this means that manufacturers are creating large, highly interconnected networks that could be vulnerable to attack without incurring significant legal liability.[65] While

62. *See* Karola V. Kreitmair, *Dimensions of Ethical Direct-to-Consumer Neurotechnologies*, 10 AJOB NEUROSCIENCE 152–166, 157 (2019) (discussing cybersecurity concerns and offering as an example "in August 2017, the FDA recalled 465,000 implantable pacemakers, because they were vulnerable to hacking, allowing malicious actors the capability of delivering inappropriately paced shocks to the heart or rapidly draining batteries").

63. Kreitmair elaborates, "Based on EEG data, scientists have been able to reconstruct images of faces that an individual is experiencing. With electrocorticography (ECoG), researchers have been able to decode the words a person is thinking to herself. Researchers have also been able to predict the propositional content of a thought sentence from functional neuroimaging (fMRI) data. While ECoG and fMRI are not functionalities of current DTC neuro-technologies, it is not clear that decoding mental content will always remain beyond the reach of consumer products." *Id.* at 159.

64. *See* Charles T. Harry, *Reminder: All those "Smart Devices are a Growing Security Threat*, FAST COMPANY (Jan. 11, 2019), https://www.fastcompany.com/90291265/reminder-all-those-smart-devices-are-a-growing-security-threat [https://perma.cc/VPF2-NSVK] ("These devices' variety means they're useful for lots of things, but also means they have a wide range of vulnerabilities. They include weak passwords, unencrypted communications and insecure web interfaces. With thousands, or hundreds of thousands, of identically insecure devices scattered all over the world, they're a wealth of targets ripe for the hacking."); *See also* Sumit Bhattacharya, *The Top Ten IoT Vulnerabilities,* INFOSEC (Feb. 17, 2018), https://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/ [https://perma.cc/LS59-EC5J].

65. Note that "These concerns are not merely speculative. By way of 'real life' example,

the risk may be negligible when applied to smart refrigerators, for example, it is of greater significance when applied in the context of consumer's brains as "connected devices."[66] Thus far, consumer disinterest and the failure of regulators has enabled manufacturers to produce connected devices that are vulnerable to security failures. However, looking to states as "laboratories" of democracy,[67] California has recently passed the first statute addressing this problem, the California IoT Law, which regulates security features of connected devices.[68] In addition to prescribing appropriate network authentication features, the statute provides that the manufacturer must include "reasonable" security features that are: appropriate for the device's nature and function; appropriate for the types of data involved; and created to prevent any "unauthorized access, destruction, use, modification, or disclosure."[69] It is provided within the same title that "'connected device' means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address"[70]

Regarding the new statute, some have criticized its lack of specificity in providing concrete guidelines to manufacturers. For example, it fails to outline specific technical requirements that manufacturers must meet in order to comply. Although it does address methods for authentication via device passwords, it does not address other vulnerabilities of IoT devices.[71] Other weaknesses of the law include the fact that software and applications

beginning September 2016, massive distributed denial of service (DDoS) attacks took down various US Internet infrastructure companies/DNS providers, leaving much of the Internet inaccessible on the east coast of the United States and incapacitating popular websites (including AirBnB, Amazon, Github, HBO, Netflix, Paypal, Reddit, the *New York Times* and Twitter, just to name a few). Originally created by three teenaged hackers, the Mirai malware responsible for the attack was specifically designed to target and infect susceptible IoT devices such as security cameras, home routers, air-quality monitors, digital video recorders and routers using a table of more than 60 common factory default usernames and passwords. These devices were turned into a network of remotely controlled bots that were used to launch the DDoS attacks which later spread globally, impacting such diverse organizations as OVH (a large European provider), Lonestar Cell (a Liberian Telecom Operator) and Deutsche Telekom. At its peak, Mirai infected over 600,000 vulnerable IoT devices." *See* Lisa R. Lifshitz, *Security by Design: California's New Iot Security Laws*, BUS. L. TODAY, (Nov. 2018), at 1, 1–2.

66. *See* Cal. Civ. Code § 1798.91.05 (West 2019).

67. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932).

68. CAL. CIV. CODE § 1798.91.04 (West 2019).

69. *Id.*

70. Cal. Civ. Code § 1798.91.05 (West 2019).

71. *See* Jeff Kosseff, *Cybersecurity of the Person,* 17 FIRST AMEND. L. REV. 343, 363 (2018) ("Although this [authentication] requirement is a good start, as security expert Robert Graham has written, it only addresses one of many vulnerabilities in Internet of Things devices.").

security are not included, post market security updates and upgrades are not regulated, and it does not provide consumers any private right of action against manufacturers.[72] From an emerging biotech perspective, it is particularly noteworthy that the legislation does not apply to devices already covered by federal oversight such as U.S. Food and Drug Administration (FDA) regulation.[73]

The current increase of data abuse and vulnerability to hackers is likely to push consumers closer to the tipping point at which they demand better privacy and security protections for the tech devices that are now so integrated into their daily lives.[74] This concern increases when health data, such as that collected by BCI devices, is being evaluated as it is even more sensitive than most other types of data, arguably even financial data.[75]

B. A Federal Proposition: The Consumer Online Privacy Rights Act (COPRA)

American consumers are increasingly distrustful of both technology companies and government surveillance. The percentage of Americans who believe that technology companies are having a positive effect has decreased from 71% in 2015 to 50% in 2019.[76] 51% believe that major technology companies should be more regulated than they are now.[77]

Despite the lobbying efforts of Silicon Valley technology companies, the Senate introduced a federal privacy bill in response to flagrant abuses of consumer data, responding to the State of California's action in passing the CCPA.[78] Democratic Senator Maria Cantwell introduced the Consumer

72. Lifshitz, *supra* note 65.

73. Lifshitz, *supra* note 65, at 3.

74. *See* Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76 (2016); Aaron Smith, *Americans and Cybersecurity*, PEW RSCH. CENTER: INTERNET, SCIENCE & TECH (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/G3X5-L7VN].

75. Kellogg, *supra* note 74, at 76 ("Health data is more vulnerable in general as a data set than financial data because you can't replace it like you can a credit card").

76. Brooke Auxier, Monica Anderson & Madhu Kumar, *10 tech-related trends that shaped the decade*, PEW RSCH. CENTER (Dec. 10, 2019), https://www.pewresearch.org/fact-tank/2019/12/20/10-tech-related-trends-that-shaped-the-decade/ [https://perma.cc/4GGG-3XTW] (last visited Feb. 5, 2020) (showing a bipartisan decrease in public sentiment towards tech companies).

77. *Id.*

78. Tony Romm, *California adopted the country's first major consumer privacy law. Now, Silicon Valley is trying to rewrite it*, WASH. POST (Sept. 3, 2019),

Online Privacy Rights Act (COPRA) on November 26, 2019, and it was referred to the Committee on Commerce, Science and Transportation.[79] As introduced, COPRA creates a variety of data rights for consumers including a right to access and transparency, a right to delete, and a right to data minimization.[80]

Some commentators have speculated that the private right of action included will be a sticking point for Senate Republicans seeking to avoid overregulating the tech industry.[81] Despite this concern for the tech industry, increased data security and privacy standards might actually be necessary to engender the consumer trust needed to allow for adoption of more advanced, but also invasive, technologies like BCI. This may be bolstered by the inclusion of a private right of action, due to consumers' distrust of government or corporations to be proper stewards of their data rights. Furthermore, there are conflicts of interest related to law enforcement accessing consumer data that is collected by private technology companies.[82] This could present a disincentive for strong government

https://www.washingtonpost.com/technology/2019/09/02/california-adopted-countrys-first-major-consumer-privacy-law-now-silicon-valley-is-trying-rewrite-it/ [https://perma.cc/G9SK-BYXQ]; Lauren Feiner, *Senate Democrats reveal new digital privacy bill that would strengthen the FTC's enforcement powers over tech companies*, CNBC (Nov. 26, 2019, 12:39 PM), https://www.cnbc.com/2019/11/26/senate-democrats-reveal-new-copra-digital-privacy-bill.html [https://perma.cc/87H7-H2U9].

79. Maria Cantwell, *Committees - S.2968 - 116th Congress (2019-2020): Consumer Online Privacy Rights Act* (Dec. 3, 2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968/committees [https://perma.cc/C8LZ-NUQS].

80. Consumer Online Privacy Rights Act, S.2968, 116th Cong. (2019). This bill fizzled out by the end of Summer 2020 as COVID-19 legislation preoccupied legislator's efforts. However, the need for federal privacy policy continues, as evidenced by the September 2020 Senate Commerce Committee hearing "Revisiting the Need for Privacy Legislation." Before the hearing, Republicans introduced the SAFE DATA Act. This Act broadly preempts state law and does not provide for a private cause of action. Thus far, it has not seemed to gain traction across the aisle. Cameron F. Kerry & Caitlin Chin, *How the 2020 elections will shape the federal privacy debate*, BROOKINGS (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/ [https://perma.cc/Z9ZV-HLJY].

81. Cat Zakrzewski, *The Technology 202: Top Senate Democrat's new privacy bill likely to spark GOP protests*, WASH. POST (Nov. 26, 2019), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/11/26/the-technology-202-top-senate-democrat-s-new-privacy-bill-likely-to-spark-gop-protests/5ddc3680602ff1181f2640e3/ [https://perma.cc/U59E-UVPY].

82. *E.g.* Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise,* N.Y. TIMES (Dec. 30, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html [https://perma.cc/P69R-53D3]; Jack Nicas & Katie Benner, *F.B.I. Asks Apple to Help Unlock Two iPhones*, N.Y. TIMES (Jan. 7, 2020) https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html [https://perma.cc/U7VE-EN57].

enforcement of any violations of the COPRA. Senator Cantwell has defended the inclusion of a private right of action against companies large enough to outmaneuver bureaucratic agencies.[83] She said "'There's nothing like the CFO, CEO and the general counsel getting in a room and going, 'You know, we could be sued for this…Guess what that changes? Behavior.'"[84]

In regard to device security, Section 107, which covers the Right to Data Security is somewhat ambiguous as to when in the data lifecycle the right begins to apply.[85] This leaves open the question of device security standards that may be required. If the trend of technology becoming increasingly integrated in the daily lives of Americans and devices becoming increasingly invasive continues, then there is a strong case to be made that federal law should not only protect data privacy with a private right of action but also take measures to protect device security as well.

III. CONSIDERATIONS FOR FUTURE DATA PRIVACY AND SECURITY POLICY

Although it can be difficult for most consumers to establish harm sufficient to gain standing in data breach cases, it would be naïve to discount the value of adequate data privacy and security.[86] As society continues to navigate the emerging Information Age, it is clear that data has immense value, but it is yet to be determined whether consumers should have any rights to that value. Additionally, as data becomes more personal and invasive, it also becomes immutable and thus more concerning when compromised. While a new credit card number can be issued, a new genomic sequence cannot.[87] Furthermore, invasive devices and highly personal data present serious opportunities for exploitation from both

83. Tony Romm, *Top Senate Democrats unveil new online privacy bill, promising tough penalties for data abuse*, WASH. POST (Nov. 26, 2019), https://www.washingtonpost.com/technology/2019/11/26/top-senate-democrats-unveil-new-online-privacy-bill-promising-tough-penalties-data-abuse/ [https://perma.cc/9LRY-7CXD].

84. *Id.*

85. Cantwell, s*upra* note 79.

86. *See e.g.,* Attias v. CareFirst, Inc., 365 F. Supp. 3d 1, 12 (D.D.C. 2019), *appeal dismissed*, 969 F.3d 412 (D.C. Cir. 2020), *and on reconsideration in part*, No. 15-CV-00882, 2021 WL 311000 (D.D.C. Jan. 29, 2021) ("the mere threat of misuse of personal information would not be sufficient to state a claim for actual damages").

87. Kellogg, *supra* note 75.

governmental action for surveillance purposes and private action for profit to name a few.[88] Although a full analysis of the risks associated with a largely unprotected invasive data profile of an individual consumer is beyond the scope of this paper, the lack of significant individual harm from data breaches thus far is not representative of potential harms going forward. As such, it is prudent to lay the groundwork with the law today to respect an individual's rights in regard to data privacy and device security.

A. Augmentative BCI is Part of a Larger Trend Towards Invasive Technology

From basic recordings of search history on Google to more sensitive recordings of an individual's location, heart rate and activity levels to their exact genomic code, there's no question that advances in technology mean that the types of data collected become increasingly personal. However, the potential adoption of augmentative BCI takes this trend to an unprecedented level. Although data privacy and security issues were pushed aside when dealing with personal computers, cell phones, and in-home smart devices, they could become much more serious threats. As such, policymakers must be considering early-stage technologies like BCI and others that could be even more invasive when crafting solutions to these issues. Based upon existing scholarship and bipartisan support for a federal privacy statute, this paper focuses upon elements that should be incorporated into a federal data privacy and device security policy, treating arguments regarding the need for such legislation as beyond its scope.[89] This section will focus on the need for a federal statute with a broad scope, sufficient enforcement mechanisms, an incorporation of device security standards, and prohibitions as needed while comparing these mandates with the existing proposal seen in COPRA.

---

88. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).

89. *See* Cameron F. Kerry, *Will this new Congress be the one to pass data privacy legislation?*, BROOKINGS (Jan. 7, 2019), https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/ [https://perma.cc/A6CG-JB8V]; Hartzog & Richards, *supra* note 88.

B. More Comprehensive Data Privacy and Security is Needed for the Information Age

Currently, there is not a sufficiently comprehensive policy framework in the United States to govern the issues of privacy and security for emerging technologies. This is certainly true when considering the highly invasive nature of BCIs which interface directly with users' brains, collecting data about an individual's neural signals, thoughts, and emotions.[90] It seems obvious that widespread adoption of this technology could have significant societal implications. The risks and benefits of that adoption will likely be varied (and to some degree unanticipated) but will certainly include the collection and processing of data of an unprecedented degree of sensitivity. The fact that technology is being developed to work with such invasive data highlights the need for a data privacy and security policy that not only deals with today's data abuses but also seeks to anticipate the protection of consumers' most personal data as the Information Age progresses.

1. The Scope Should Allow for Dynamic Regulation

Technology in the Information Age is known to advance rapidly and present new challenges for lawmakers.[91] These challenges are especially salient given the drastic differential in economic power and technical knowledge between large technology companies and individual users.[92] Because potential abuses are varied and likely to continue evolving rapidly, any federal statute should be sufficiently broad to allow for dynamic regulation through agency guidance and caselaw development.[93] This regulatory power should be granted to either an existing agency or to a new agency created specifically for the purpose of governing data privacy and cybersecurity. Doing so will create a more dynamic regulatory environment

90. *See supra* Part II, *see also* notes 63, 115 and accompanying text.
91. *E.g.*, Tricoles, *supra* note 27.
92. Hartzog & Richards, *supra* note 88.
93. ". . . there's a strong case for governments to innovate in the regulatory space in a way that's like innovation in the tech sector itself. Instead of waiting for every issue to mature, governments can act more quickly and incrementally with limited initial regulatory steps—and then learn and take stock from the resulting experience." Brad Smith & Carol Ann Browne, *Tech Firms Need More Regulation*, THE ATLANTIC (Sep. 9, 2019), https://www.theatlantic.com/ideas/archive/2019/09/please-regulate-us/597613/ [https://perma.cc/LB4G-WDMT].

that will allow the law to better adapt and tackle new threats to data privacy and security as they arise. Criticisms of a broad regulation of data privacy have been advanced, namely in response to the GDPR. These criticisms often lament the increased costs to businesses, express concern for the tradition of "free and open exchange of information" on the Internet, and suggest that regulating this exchange might lead to less innovative technology.[94] Although these concerns are legitimate and an appropriate balance will need to be struck, there is currently a much greater risk from a total lack of regulation.[95] Furthermore, broad legislation with dynamic regulatory guidance will allow companies to look to agency recommendations for clarity and guidance in developing and maintaining proper privacy and security for new innovations. This may help to mitigate any worry about legislative changes which could negate the viability of technologies that companies have invested significant amounts of capital in developing. Allowing protections to develop through caselaw and under iterative regulatory guidance can help to lessen any potential drag on innovation and increase compliance. It will also help to better protect consumers' privacy security by lessening the likelihood of powerful technology companies finding work arounds for static prohibitions.

COPRA is a strong step in the right direction; however, it is somewhat limited because it primarily seeks to protect data by placing limitations upon known abuses. For example, the right to data security seems meant to address data breaches[96] and the right to access and transparency seems to seek to ensure that consumers are operating with more complete information about their data and how it is being used.[97] This format is limited by its enumeration of specific rights, in an attempt to prevent already known abuses, and by its assignment of enforcement responsibility to consumers.[98] The average consumer does not have the time or inclination to download,

94. *See* Adam Satariano, *Europe Is Reining In Tech Giants. But Some Say It's Going Too Far.*, N.Y. TIMES, (May 6, 2019), https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html [https://perma.cc/8CWL-JC4M]; Larry Downes, *GDPR and the End of the Internet's Grand Bargain*, HARV. BUS. REV. (Apr. 9, 2018), https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain [https://perma.cc/FA6N-FURX]. *But see* Smith & Browne, *supra* note 93.

95. The President of Microsoft wrote "And it's not that governments will move too fast. It's that they will be too slow. Technology innovation is not going to slow down. The work to manage it needs to speed up." Smith & Browne, *supra* note 93.

96. S. 2968, 116th Cong. (2019).

97. *Id*. § 107.

98. *See also* Hartzog & Richards, *supra* note 88.

read, verify, and monitor how every data point is being used. Companies should not be able to misuse increasingly sensitive data merely due to a lack of consumer oversight. One example of a more broadly-written provision is the duty of loyalty that COPRA places on covered entities prohibiting deceptive or harmful data practices or any other violation of the Act.[99] A statute written with more emphasis on broader affirmative duties for companies or general prohibitions to be fleshed out by regulators could be more effective in providing a framework for adaptable, relevant data privacy and security policy moving forward.

Importantly, COPRA provides for the establishment of a new Bureau within the Federal Trade Commission (FTC) for addressing "privacy, data security, and related issues."[100] This is a great strength of the legislation and should allow for more dynamic regulation in a rapidly evolving space. Additionally, this unnamed Bureau will be able to develop some expertise in data and technology in order to work with the industry to offer guidance moving forward, which is likely to improve compliance and the development of sustainable regulation that does not stifle innovation.[101]

2. Sufficient Enforcement Mechanisms Necessary

In order to have the intended impact, any legislation should have adequate mechanisms for enforcement. This should include a private right of action in order to incentivize compliance by corporate entities without requiring consumers to rely entirely upon regulatory enforcement. This is due to the frequency with which powerful companies have been able to maneuver around bureaucratic enforcement[102] and because there are instances where the government has an interest in a company "compromising" its privacy standards to some degree.[103] The latter is likely more of a constitutional issue which is beyond the scope of this Note but will need to be worked out by the courts and by policymakers. However, this concern still supports extending a private right of action to consumers. A private right alone, however, could be insufficient due to the power

99. S. 2968, 116th Cong. § 101 (2019).
100. *Id*. § 301.
101. Smith & Browne, *supra* note 93.
102. Romm, *supra* note 83.
103 Hill & Murphy, *supra* note 82; Nicas & Benner, *supra* note 82.

differential between consumers and large technology companies which makes some private claims impracticable due to their cost. Further, most consumers lack the requisite amount of time and technical expertise to monitor companies' data practices.[104] As such, enforcement authority should be vested in either an existing regulatory agency or a new agency created for the express purpose of governing data privacy and cybersecurity. Additionally, State Attorneys General should have the power to enforce the legislations requirements through some cause of action as well.

Because COPRA provides for the formation of a Bureau to aid in enforcement as well as for civil enforcement, it includes a sufficient degree of governmental enforcement.[105] Furthermore, it allows for private rights of action in violations of certain provisions.[106] Therefore, the bill includes both public and private mechanisms, a key element of a strong data privacy and device security policy.

3. Device Security Standards

Device security is an integral component of the safety and privacy of users. As such, a federally mandated standard of requisite device security should be incorporated into the legislation.[107] Unlike the California IoT Law, federal standards should be specific enough to allow the private right of action mentioned above to apply.[108] The difficulty of proving damages in a case of failure to comply with security standards is likely to provide an adequate check to prevent this cause of action from being used excessively by plaintiffs, although this would be decided to some degree by the courts.[109] Furthermore, the standards should remain sufficiently broad to allow for rapid updates in industry cybersecurity standards. Once again, the proper

104. Hartzog & Richards, *supra* note 88.

105. S. 2968, 116th Cong. §§ 301(a)(1), (b) (2019).

106. S. 2968, 116th Cong. § 301(c) (2019).

107. Device security refers to measures taken to protect data that is collected, stored, transmitted, and processed by devices in order to prevent unauthorized access. *See e.g.* Mobile Device Security, VMWARE, https://www.vmware.com/topics/glossary/content/mobile-device-security [https://perma.cc/63BL-DZAU] (last visited May 25, 2021).

108. CAL. CIV. CODE § 1798.91.04 (West 2019).

109. Christopher Escobedo Hart, Peter Sullivan, & Colin Zick, *In Cybersecurity, No Harm Does Not Necessarily Mean No Foul*, JD SUPRA, https://www.jdsupra.com/post/contentViewerEmbed.aspx?fid=eec1ea97-ee3e-4a77-9a61-07719323a590 [https://perma.cc/7EUQ-F3RJ] (last visited Jun 20, 2021).

agency should be able to further regulate these standards.

COPRA is focused mainly on companies collecting and processing data. The bill does provide for a right to data security but does not include device security measures.[110] Because COPRA solely focuses on actions taken by companies to ensure the integrity of the data that they may store and process, it overlooks device security, which is often the initial point of data collection.[111] Although this point in the life cycle is most vulnerable to malicious third parties, companies should still bear some responsibility for ensuring adequate security at this phase if they will be collecting highly sensitive data from consumers. This continuing gap in the safety and integrity of consumer technology should either be addressed by the FTC Bureau that is created or ideally, referenced more explicitly in the bill. Device security is a crucial first step in the collection of consumer data and thus too important to data privacy and consumer protection to be excluded from the policy. While the California IoT Law could be used as a starting point for this inclusion, mandating security updates and providing some guidelines for software and applications security would also be important when ensuring the security of consumer technology devices and the data that they could collect.[112]

4. Highly Sensitive or Invasive Data Points

There are serious technical limitations to permanent deletion of data. This is due in part to cloud storage, the scale of server storage, and a general lack of clarity surrounding permanent deletion.[113] Although not insurmountable, ensuring full deletion is not always economically feasible. Some companies even create carve-outs in the data destruction section of their Non-Disclosure Agreements to allow for retention of data that has been backed up to its servers for this reason.[114] Because of this and the relative

110. S. 2968, 116th Cong. § 107(c) (2019).

111. Jahoon Koo et. al., *Security and Privacy in Big Data Life Cycle: a Survey and Open Challenges*, 12 MDPI SUSTAINABILITY 1, 3 (2020).

112. *See also* Lifshitz, *supra* note 65.

113. Steven Melendez, *Making Sure Deleted Data Is Really, Truly Gone*, FAST COMPANY (Nov. 24, 2015), https://www.fastcompany.com/3053316/making-sure-deleted-data-is-really-truly-gone [https://perma.cc/9D6P-A2WC].

114. Catherine Bragg, *Non-Disclosure Agreements in Review*, AM. BAR ASS'N (Aug. 20, 2019), https://www.americanbar.org/groups/construction_industry/publications/under_construction/2019/summer/non-disclosure-agreement/ [https://perma.cc/XX46-2QX5].

inability of the average consumer to verify that all traces of his or her data have indeed been deleted, there may be some types of data that merit total protection from ever being collected in the first place.[115]

It is likely that as devices become more invasive and the data collected becomes increasingly sensitive, there could be a threshold at which it may be necessary to completely ban the collection of said data types. Other protections such as notice and control will simply be insufficient due to the high potential for abuse, which at a certain point will outweigh any legitimate business uses such as research and development, enhancing user experience, etc. The policy should allow for this power subject to serious inquiry and at the discretion of the agency charged with data privacy and security. If compliance is a serious concern, criminal sanctions may be appropriate to include as well.

Although COPRA includes a right to data minimization, a right to deletion, and limits upon the processing and transfer of certain data points relating to an individual's civil rights, it fails to provide any option for more comprehensive restrictions upon companies, barring the collection of certain data types.[116] While this is unsurprising as the bill was likely written with modern technology companies in mind, it should still allow for the possibility that the FTC Bureau charged with this issue may see fit in the future to disallow any collection. For the aforementioned reasons, a right to deletion may not always be sufficient protection for highly sensitive data such that may be collected by invasive technologies like BCI.

---

115. As an example of data that may warrant total protection from collection, consider neural data. Because neural data can be used to record thoughts, attention levels, emotional states, and possibly even memories, this deserves especially serious consideration for policies governing BCIs. *See, e.g.,* Jeremy Greenberg & Katelyn Ringrose, *Five Top of Mind Data Protection Recommendations for Brain-Computer Interfaces*, FUTURE OF PRIV. FORUM (May 4, 2021), https://fpf.org/blog/five-top-of-mind-data-protection-recommendations-for-brain-computer-interfaces/ [https://perma.cc/U8RS-H8XK]; Alexandre Gonfalonieri, *What Brain-Computer Interfaces Could Mean for the Future of Work*, HARV. BUS. REV. (Oct. 6, 2020), https://hbr.org/2020/10/what-brain-computer-interfaces-could-mean-for-the-future-of-work [https://perma.cc/BB6K-SH9H].

116. S. 2968, 116th Cong. §§ 106, 103 (2019).

C. Balancing with Commercial Interests and Technological Innovation

As discussed, there are legitimate concerns regarding the establishment of a strong federal policy regulating technology companies which could potentially inhibit innovation and future growth in a critical sector.[117] Additionally, many technology companies use much of the wealth that they collect in consumer data to tweak their applications in order to offer an enhanced user experience, making the technology more valuable to consumers and to society. Without the ability to collect and analyze data, technological development may be hampered.[118] These are legitimate concerns and it would be advisable for the FTC Bureau charged with regulating data privacy and security to balance these concerns with those of consumer protection and the integrity of the data privacy framework. There may eventually need to be a classification system or some other means of distinguishing between less sensitive consumer data and highly invasive consumer data, each of which would obviously weigh differently against the interests of businesses and innovation.[119]

Many of the more stringent elements suggested here are defensible in relation to a technology as invasive as BCI but could be considered over-regulation for some less invasive types of technology. However, it would be inappropriate to rely upon sector-specific legislation (such as HIPAA) to regulate invasive biotechnology data. This is because of the potential for abuse as seen in emerging consumer health companies often falling outside of relevant HIPAA restrictions.[120] Overall, it is important to have a dynamic policy shaped by agency guidance and rulemaking as discussed above in order to quickly adjust to evolving threats posed by rapidly changing technology.

---

117. Zakrzewski, *supra* note 81.

118. *See supra* Part II.

119. *See also* Carpenter v. US, 138 S. Ct. 2206 (2018) (some forms of highly personal data, like cell phone location data, deserve greater protection).

120. Parker et al., *supra* note 61.

CONCLUSION

BCI is an emerging biotechnology that could allow elective brain augmentation. This is an extreme but logical extension of the existing trend towards invasive consumer technology products. From stationary desktop computers to portable laptops to smart phones which have essentially become fifth limbs for many of today's consumers[121] to the Internet of Things (IoT) devices that are becoming increasingly prevalent in homes (e.g., Alexa, Nest, smart refrigerators, doorbell cameras, etc.), connected devices—and the data that they collect—are becoming integrated into more and more aspects of consumers' daily lives.

The data privacy and security concerns that accompany these devices are significantly greater if consumers are willing to adopt invasive BCI for augmentative purposes as some technology companies are hoping. The need for adequate data privacy protection will become highly relevant as these BCI devices will be collecting data on consumers' neural signals – gleaning access to their most private thoughts and fleeting emotions.[122] Even if BCI does not attain widespread adoption, the overall trend towards invasive technology collecting increasingly personal data means that Congress should be intentional about crafting federal privacy and security legislation that is equipped to handle these challenges moving forward rather than merely addressing privacy abuses that have been seen thus far. The rapid pace of technology development and high potential for consumer abuse and infringements upon privacy for surveillance purposes necessitate it.[123]

Establishing a dynamic framework for federal data privacy and device security policy is an important first step in equipping the law to handle the technological developments yet to come. Key elements of this include a broad statute that adequately equips an agency to develop adaptable regulations, sufficient enforcement mechanisms to promote compliance, incorporation of device security standards in order to ensure data safety from the initial point of collection, and an allowance for possible prohibition of collecting certain data types due to the realities of digital storage. COPRA recognizes some of these elements but falls short when it comes to others. It rightly provides for the establishment of a new Bureau within the FTC to

121. Urban, *supra* note 22.
122. Warren & Brandeis, *supra* note 53.
123. Hartzog & Richards, *supra* note 88.

handle data privacy and related matters.[124] This will allow for more dynamic regulation and more attentive enforcement. However, the rights provided for in the bill seem to be primarily based upon data privacy abuses that have already been discovered without offering adequate breadth to allow the new Bureau to quickly adapt to emerging issues with newer technology and data types.[125]

In regard to enforcement mechanisms, COPRA seems to provide for sufficient enforcement to encourage compliance, ideally without overburdening technology companies. COPRA does not offer any guidance on device security or allow for special treatment (such as prohibiting collection) of overly invasive data types that may be seen in the future.[126] As such, COPRA is an important step towards a federal framework for data privacy but fails to adequately anticipate the future likelihood of increasingly invasive consumer technology. Laying a broad and iterative regulatory framework in the near-term will allow policymakers to better handle the rapid developments of invasive consumer technologies over the long-term. Therefore, the legislative elements proposed in this paper for addressing the concerns presented by BCI are by no means comprehensive but should nevertheless be seriously considered as components of a truly forward-looking data privacy and device security policy equipped to handle the development of BCI and beyond.

124. S. 2968, 116th Cong. § 301(a) (2019).
125. Hartzog & Richards, *supra* note 88.
126. S. 2968, 116th Cong. (2019).