Protecting the Brain:

Analyzing the Capabilities and Vulnerabilities of Brain-Computer Interfaces

Diana Sapashnik

Tufts University, Fall 2019

Abstract

Brain-computer interfaces (BCIs) can interpret movement, speech, and images, digitizing what are among the most sensitive personal data that we as individuals generate. With the commercialization of EEG BCIs and the emergence of new, potentially consumer-friendly BCI technology from Neuralink, the availability and widespread transfer of this data is likely to increase substantially. As such, it is very important to consider that software used for BCI acquisition and storage must be developed with best security practices in mind before BCIs gain popularity. It is also pertinent to establish legislation to protect consumer's rights and stay ahead of this fast-moving field.

1. Introduction

A brain-computer interface is a system that records brain signals and interprets them into actions, emotions, images or speech[1]. Brain waves are recorded using electrodes that measure an electric field surrounding a firing neuron[2]. Neurons fire off signals only when enough neurotransmitters coalesce at the end of a neuron's axon to overcome an electric action potential. Overcoming the energy barrier releases the neurotransmitters into another neuron and the signal triggers a chain reaction of information. This information is recorded by BCIs as an oscillating series of discrete signals, which are deconvoluted using machine learning methods such as deep or convoluted neural networks.

Research in BCIs has demonstrated a wide set of uses, including control over motion and interpretation of words and images. They can be used to move mouse cursors in two dimensions, open applications, and type characters onto a screen[3, 4]. Prosthetics can be fit onto amputee limbs, and the bending of fingers and elbows can be controlled by focusing while wearing a electroencephalogram (EEG) headset[5]. Researchers at USCF, in an effort funded by Facebook, were able to interpret brainwaves and decode simple answers to questions[6]; and deep neural networks were successfully leveraged to partially reconstruct images of animals[7].

BCIs have mainly been used in research laboratories and hospitals. However, as humans become increasingly dependent on their devices, the demand for safe, portable coupling between user and machine is growing. With the emergence of lightweight hardware, surgical robots, and artificial intelligence, the possibility of the average consumer communicating with computers solely by thinking grows more likely. EEG headsets are already on the market for gamers. Next year, Neuralink intends to start its first in-human clinical study of its own BCI. The study is currently recruiting patients with motor impairment but has public plans to pivot to healthy patients[2]. With brain-wave sensors becoming more mainstream, there will be a trove of data

available to train machine learning algorithms with the potential to further enhance communications between human minds and computers. The ability to mine and interpret brain biometrics, though remarkable for its potential to improve quality of life, also threatens to break down the biological barriers between the human mind and public access by digitizing brain waves. As this technology continues to advance at an increasing rate of development, careful forethought is needed in determine best practices for securing sensitive data by proactively mitigating software vulnerabilities. It is also appropriate to question how prepared current legislation is to protect user sensitive brain biometrics to stay ahead of the curve of a rapidly changing society.

2. To the Community: Think Like a Futurist

Biometric data is of high value for countries, companies, and individual attackers alike because of the breadth of information they hold. While currently only limited (but important) information can be inferred from brain signals, current leaps in BCI technology mean that there is great potential for unexpected advances in the field. Additionally, given the rapid pace at which technological developments revolutionize societal structures, epitomized in the Fourth Industrial Revolution, it is a worthwhile exercise to think like a futurist. Trying to anticipate the consequences of new technology is increasingly important. Upon the invention of the Internet, there was likely little thought given to the possibility that social media platforms would one day be a source of political turmoil. By the time the public was alerted to the severity of the issue it became too complex to easily fix. Securing biological data is already a high-priority issue, as is passing laws to protect user data. However, before BCI technology can progress to new levels of sophistication, it is prescient to anticipate the early ethical implications and establish legal protections such as freedom of thought, a human right that in the past could not be violated.

3. Consumer BCIs and Beyond

3.1 Electroencephalogram (EEG)

There are numerous types of brain-computer interfaces, but two in particular have significant potential to broadly impact society given their number of already commercialized and distributed products. The first are electroencephalograms (EEGs), which are a series of electrodes placed on a user's head. EEG gaming headsets, EPOC and MindWave, are available for the public at a few hundred dollars each[8, 9]. Other commercially available EEG caps, such as SmartCaps or Neuro Cap devices, are utilized to monitor emotional state and mental focus[10]. Nissan is working on its own implementation of an EEG-based brain-computer interface to attempt to monitor driver focus and visualized steering[11].

The EEG's popularity is rooted in its portability and ease of use. Due to its noninvasive nature, a user can avoid costly hospital visits and unintended health side effects that can occur from procedures in which electrodes are implanted directly into a user's brain. Such invasive procedures pose risks of blood vessel rupture and concern with electrode degradation over time, especially as waste products are not easily removed from brain tissue. The safety and convenience of EEGs come with the cost of noisy, convoluted brain biometrics, as it manages signals from many neurons rather than specifically measuring a certain subset. Additionally, wearable EEGs make use of dry electrodes rather than gelled electrodes utilized in medical grade EEGs, causing

at times unreliable and inaccurate data aquisition[12]. EEG sensors also pick up additional electrical activity outside of brain waves, such as blinking or jaw clenching, resulting in a false positive of signal[13]. As such, it's unlikely that EEG caps used to monitor workers in China or Australia can accurately detect a worker's level of anxiety, depression or focus, however it speaks volumes that wearable technologies to monitor workers' emotions, though imperfect, are still in use.

There is a concerted effort to minimize noise in EEG signal through algorithmic artifact removal and advancements in machine learning models[14]. It's possible that all the necessary data is already available in EEG graphs, and more invasive methods are not necessary to reduce the noise in signal. Separately, Elon Musk's Neuralink has made strides in developing a potentially safe and convenient way to surgically implant electrodes much closer to neurons, which might provide the specificity necessary to collect more in-depth information on the brain.

3.2 Neuralink

Neuralink, a neurotechnology company that develops brain-computer interfaces, published its advances in surgical precision and increased bandwidth of a BCI, as well as announced its intentions for first in-human trials for 2020. The device used to measure brain signals, called the N1 implant, is a polymer probe equipped with more than a thousand electrodes, whereas typical BCIs for motor and speech control have up 250 electrodes[15]. Each electrode is very small, roughly the size of a neuron each, and for accurate and precise insertion Neuralink developed a robot to handle electrode implantation. The electrodes extend from a chip that fits behind a subject's ear, and the measured signals are wirelessly transmitted to a phone via Bluetooth[2].

The surgical robot was designed with patients' comfort in mind. Traditional invasive methods for implanting devices into the brain are unlikely to attract a large cohort of users. Neuralink attempts to improve patient experience by minimizing the complexity of the surgery. The surgery is kept on a small scale by utilizing a small hole drilled into the skull for thread insertion, and takes 45 minutes to complete. The intent is that with the precision of the robot and the small entry for implantation, patients will be more comfortable with the medical procedure.

With thousands of electrodes in the N1 for accurate and distributed measurement, as well as a surgical robot for a simplified surgery, these new advances have the potential to change the landscape of the interpretation of brain signals, as well as attract users outside of a clinical setting. There are more obstacles and data needed before such a reality is assured, such as long-term studies of electrode stability and robot accuracy. While this research and development of commercialized BCIs is in its infancy, this is the exact time to ensure that these new technologies are being developed with best security practices in mind and to craft legislation to meet the possible applications of widespread use of increasingly accurate and precise BCIs.

4. Best Security Practices

4.1 Static Analysis and Penetration Testing

To ensure the security of emerging BCIs, companies that develop software for sensors and transmission, particularly ones that collect brain waves, should have protocols in place for static analysis and penetration testing prior to systems deploying. Published code weaknesses and vulnerabilities of existing EEG devices suggest that such practices are not always in place. In 2016,

Alejandro Hernandez, a consultant at IOActive, demonstrated at DEFCON successful man-in-the-middle and denial of service attacks across three different EEG devices and acquisition software[16]. In his review of technical manuals and specifications of EEG devices and software, the majority contained no mention of security, cryptography, or authorization, demonstrating that much of the software developed up to that point was without security in mind, leading to weaknesses in source code that went undetected. In 2017 Cisco Talos, a security threat research team, conducted a review of Natus' Neuroworks software, which connects with EEG devices and interacts directly with user data. Five vulnerabilities were uncovered: four buffer overflow weaknesses and an opening for a denial of service attack[17]. Buffer overflow vulnerabilities allow attackers reading and writing access to restricted memory, while denial of service leads to systems becoming overwhelmed and slowing down or crashing. In 2018, researchers at Carnegie Mellon uncovered a possible implementation of Bluetooth where encryption parameters did not have to be validated, leading an opening of an adversary to intercept Bluetooth transmission, decrypt messages, and inject their own malicious content into the communication if they are within 30ft of the target[18]. As Neuralink, EPOC and Mindwave all use Bluetooth, ensuring that no steps are missed in correctly configuring encrypted transmissions in Bluetooth is essential[19].

A great way to detect weaknesses in source code is automated static analysis. Static analysis has 100% code coverage and can capture weaknesses such as buffer overflow and denial of service threats. Platforms that offer automated static analysis services, such as Veracode and Fortify, can scan source code and produce a report listing lines of vulnerable code. Additionally, hiring red team ethical hackers to attack the software would also uncover security holes, such as possible missing cryptographic steps and man-in-the-middle interjections. Performing both static analysis and penetration testing will help validate the security of BCI devices.

4.2 Multi-Factor Authentication

An additional best practice when considering storage of sensitive data is establishing multi-layer authentication. Interestingly, the use of EEGs themselves could be a novel way to make multi-factor authentication even more robust against attacks. Multi-factor authentication relies on three things: something a user has, something a user knows, and something a user is[20]. The 'is' requirement is any sort of biometric data such as facial identification, fingerprints, retinal scans or a combination.

Even though it's challenging to bypass MFA, it's still possible. An attacker can intercept a PIN sent to a device, crack a password, or trick a user to disclose PINs and passwords. As for biometric validation, that is only secure until it's cracked or leaked, and then it's useless. Recently, the fingerprints of more than a million users were exposed, and those users could no longer securely use their fingerprints for authentication of any device[21]. Although it's challenging for an attacker to take advantage of possible weaknesses in every layer of MFA, it's possible to make it even more impractical for them to try. Researchers at Elsevier found that using brain wave recordings as a new layer of biometric security is possible[22]. Users' brain waves were recorded while focusing on three images. Each user's brainwaves are slightly different, generating a unique identification. As little as three electrodes were necessary for reliability, reducing the amount of information necessary for EEG-level passwords. Should a data breach leak expose EEG data, users can simply record signals generated from concentrating on three new images, which will generate the equivalent of a new unique password. The infancy of consumer BCI development not only

gives developers a chance to practice strong security foresight before widespread use, but also offers engineers new security methods using this pioneering technology.

5. Legal Protections from Companies and Countries

5.1. User Data Protections

There are numerous other recommended practices to secure data integrity. Discussed here are several key methods to keep in mind when developing software for brain biometric collection and storage. However, no amount of good security practices addresses the ability of companies to legally sell user data or countries to use it against its constituents. The only way to truly secure brain biometrics is by passing laws that protect consumers and look ahead to protect the future implications of capturing and interpreting more sophisticated thoughts.

To date there is no comprehensive law in the United States that prohibits companies from selling or buying biometric data. There are user protection laws on the state level, such as Illinois Biometric Information Privacy Act (BIPA)[23]. Importantly, the law specifies that businesses must obtain informed consent to collect biometrics and cannot profit off them. States such as Texas and Washington have followed since with similar laws. In 2020, the California Consumer Privacy Act (CCPA) will go into effect, a sweeping new piece of legislation that has been presented as a potential model for a national law[24]. It goes beyond current laws by allowing users control over all data, not only biometrics, that's collected about them. Users must know what data is being collected about them, if it's being sold, and have the right to say no to the sale. Considering social media conglomerates' public moves to further invest in BCI technology, such as Facebook's recent acquisition of CTRL-Labs, a BCI start-up, passing such legislation is timely and relevant.

5.2 Ethical Concerns

Beyond protections of users' data from sales are deeper ethical questions surrounding BCIs. Nita Farahany, a law and philosophy professor at Duke University and a leading bioethicist expert, has begun to outline some important considerations for a future where governments have the ability to monitor the emotions and possibly thoughts of their constituents[25]. She points out that while our Constitution protects freedom of speech and religion, there is no explicit protection of freedom of thought. While some legal minds would argue thought is implicit to speech and religion, others could just as easily point to the fact there is no amendment where that is explicitly written.

Nita talks about workers' rights, referencing the EEG headsets reported to monitor factory workers and train drivers of the Beijing-Shanghai high-speech focus. As of now there are no legal protections that keep workers from being sent home should they be deemed too unfocused or emotionally unstable. In some ways, monitoring a person's focus when performing a high-stakes job could a great idea. Should someone be too fatigued or stressed to perform a task that, if incorrectly executed, could hurt people, alerting the user and letting them rest first would be great. On the other hand, there is no discrimination law prohibiting an employee being sent home and possibly eventually fired for being deemed emotionally unstable and unfocused, even if he has gone through a traumatic event such as a loved one dying.

Within Nita's talk she touches on government surveillance. An Iranian-American, she mentions restricted communications she had with family members in Iran during the Iranian Green Movement, and considers what would happen if authoritarian governments obtained access to dissidents' thoughts. She also asks about American surveillance and crafting a law to stop the NSA from spying on citizens.

Outside the scope of her talk, we might also start to consider if brain-wave interpretation should be admissible in a Court of Law. It could be potentially used to prove intent or confirm if a person is lying on the stand. Certain thoughts might also be taken out of context or misinterpreted, leading to a false rate of convictions. Debating and determining the legality of these thorny issues could help plan for future legislation in a reality where such laws would be desperately needed.

6. Conclusion

Evaluation of current brain-computer interfaces, particularly consumer-grade devices, show that we are nowhere near being able to read someone's mind. However, ongoing research into existing devices and new technology opens the door for possible rapid advancement. As a society we are currently facing an overwhelming amount of issues which could arise due to lack of appropriate security controls and legal foresight. Now that we are aware of the rate at which new technologies advance, it is imperative that we anticipate future consequences and avoid repeating our past mistakes.

References

1. Anderson, Charles and Bratman, Jeshua, “Translating Thoughts Into Actions By Finding Patterns in Brainwaves” https://pdfs.semanticscholar.org/05ea/b15811bb3289846d653c2254308a1210a210.pdf
2. Stephen Shanland, “Elon Musk says Neuralink plans 2002 human test of brain-computer interface” – link to Neuralink presentation video https://www.cnet.com/news/elon-musk-neuralink-works-monkeys-human-test-brain-computer-interface-in-2020/
3. Shih, Jerry, “Brian-Computer Interfaces in Medicine” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3497935/#bib8
4. Rezeika, Aya. “Brain-Computer Interface Spellers: A review” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5924393/
5. Nathan Shiva, “The Arduino Prosthesis Using the Neurosky Mindwave” http://learn.parallax.com/educators/inspiration/arduino-prosthesis-using-neurosky-mindwave
6. Moses, David, “Real-time decoding of question-and-answer speech dialogue using human cortical activity” https://www.nature.com/articles/s41467-019-10994-4
7. Shen, Guohau. “Deep Image reconstruction from human brain activity” https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1006633
8. Jane McGrath, “How the Emotiv EPOC Works” https://electronics.howstuffworks.com/emotiv-epoc4.htm
9. Rytis, Maskeliunas, “Consumer-grade EEG devices: are they usable for control tasks?” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4806709/
10. “Mind-reading technology is closer than you think” https://www.fastcompany.com/90388440/mind-reading-technology-is-closer-than-you-think
11. “Brain-to-Vehicle” https://www.nissan-global.com/EN/TECHNOLOGY/OVERVIEW/b2v.html
12. Ratti Elena, “Comparison of Medical and Consumer Wireless EEG Systems for Use in Clinical Trials” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5540902/
13. Angela Chen, “Brian-scanning in Chinese factories probably doesn’t work – if it’s happening at all” https://www.theverge.com/2018/5/1/17306604/china-brain-surveillance-workers-hats-data-eeg-neuroscience
14. Omelianenko, Iaroslav. “Applying advanced machine learning models to classify electro-physiological activity of human brain for use in biometric identification” https://arxiv.org/pdf/1708.01167.pdf
15. Elon Musk and Neuralink, “An Integrated Brain-Machine Interface Platform with Thousands of Channels” https://www.documentcloud.org/documents/6204648-Neuralink-White-Paper.html

16. Alejandro Hernandez, “Brain Waves Surfing: (In)security in EEG (Electroencephalography) Technologies https://ioactive.com/wp-content/uploads/2016/02/Brain20Waves20Surfing20-2028In29Security20in20EEG2028Electroencephalography2920Technologies.pdf
17. Talos, “Vulnerabilities Spotlight:Natus Neroworks Multiple Vulnerabilities” https://blog.talosintelligence.com/2018/04/vulnerability-spotlight-natus.html
18. Carnegie Mellon University, “Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange” https://www.kb.cert.org/vuls/id/304725/
19. Hassib, Mariam, “Brain Computer Interfaces for Mobile Interaction: Opportunities and Challenges” http://delivery.acm.org.ezproxy.library.tufts.edu/10.1145/2800000/2794309/p959-hassib.pdf?ip=130.64.11.161&id=2794309&acc=ACTIVE%20SERVICE&key=AA86BE8B6928DDC7%2E4579F4D1C4C67060%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1576245265_602727c17cc677d61044d6ffb50870e3#URLTOKEN#
20. Matt McDermitt, “Why Multi-Factor Authentication (MFA) is a Must-have in the Microsoft World and Beyond” https://www.business2community.com/cybersecurity/why-multi-factor-authentication-mfa-is-a-must-have-in-the-microsoft-world-and-beyond-02245731
21. Jon Porter, “Huge security flaw exposes biometric data of more than a million users” https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data
22. Ruiz-Blondet, Maria, “Permanence of the CERECRE brain biometric protocol” https://www.sciencedirect.com/science/article/abs/pii/S0167865517301940
23. Bambauer, Jane, “BIOMETRIC PRIVACY LAWS: How a Little-Known Illinois Law Made Facebook Illegal” https://pep.gmu.edu/wp-content/uploads/sites/28/2017/06/Biometric-Privacy-Laws-FINAL_really_6.20-.pdf
24. Gemalto, “Biometric data and data protection regulations (GDPR and CCPA)” https://www.gemalto.com/govt/biometrics/biometric-data
25. Nita Farahany, “When technology can read minds, how will we protect our privacy?” https://www.gemalto.com/govt/biometrics/biometric-data