A look at BCIs on the subject of Privacy

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Joseph Sam

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Joshua Earle, Department of Engineering and Society

<center>**STS Research Paper**</center>

Introduction:

As the technology of Brain-Computer Interfaces (BCI) becomes more advanced, the prospect of a BCI capable of transcribing pure human thoughts into text, images, or video is becoming more of a reality. And as a part of this advancement, there is an underlying threat to a crucial part of the human condition: our privacy. Up until this technology is developed, we can all agree that the thoughts inside of our head, for better or for worse, are ours alone. Only through our own volition, can others know what we think as we express it. And this control is something that we all value. First and foremost, it provides protection. Things we fear may draw judgement, and potential social alienation, we keep private. But its not just to protect ourselves, but also others. A parent may keep their financial worries private from their children, to avoid spreading anxiousness. So, as we progress towards a reality where this privacy can be uncovered without the voluntary action of its owner, this creates a wide array of problems. But this also creates a wide array of opportunities.

In this essay I will evaluate the pros and cons of this potential privacy invasion. I will discuss why we desire privacy to begin with and argue that BCIs don't undermine our privacy substantially more than current societal practices already do. To begin, I first explore why we value privacy, before transitioning into the state of privacy invasion in its current form, then finishing with how much more BCIs could contribute.

Part 1: Why do we all value privacy?

To understand why we value privacy, it is important to understand what privacy even is. As best stated by Daniel J. Solove in A Taxonomy of Privacy "Privacy is the relief from a range

of kinds of social friction" (Solove, 2006). Essentially, the line of thought is that privacy is derived on an individual basis out of the social friction presented by engaging in society. In order to protect yourself from the many activities that you, institutions, and governments engage in, all of which can have real and meaningful impacts on your life, you created privacy. In arguing this, there are different classifications of privacy depending on the social actors involved, and therefore, different breaches of said privacy. You likely wouldn't equate a newspaper reporting the names of victims without their consent to be breaching the same sort of "privacy" as being strong-armed into revealing personal information. Solove defined the different classifications of privacy, based on how they are breached. They are Information Collection, Information Processing, Information Dissemination, and Invasion. The right to control these 4 classifications is what we define as the right to privacy.

Now that I have established a basis of what this idea of privacy is, it is still necessary to identify what it does for us. How exactly does privacy protect us and provide relief from social friction? According to Trina Magi, a well-respected professor and former ALA Intellectual Freedom Committee member, there are 14 distinct protections that privacy offers. These protections include the protection of the opportunity to relax and concentrate. Affirmation of self-ownership and ability to be a moral agent. Prevention of the intrinsic loss of freedom of choice. Protection from self-censorship. Protection from discrimination. Protection from being misjudged out of context. Protection over control of the artifacts that support the narrative of their life. Protection of the chance to start anew. Protection of authenticity. Protection of intimacy and relationships. Protection of the Common Good. Protection from power imbalance between the individual and governments or institutions. Protection of Political Activity and Service. And lastly, protection of disagreement (Magi, 2011). These protections are further

explained and elaborated upon, but they can be categorized and simplified into 3 primary categories. They are protection of self, protection of personal relationships and protection of societal relationships. In summary, these protections are what enable us to freely be ourselves. They allow you to maintain ownership over who you are without being discriminated against or penalized. They allow you to selectively reveal yourself to those whom only you trust, and they allow for the birth of new ideas free of scrutiny until they are ready.

Part 2: What are BCIs?

Now that we have discussed briefly, what privacy is and what it does for us on both an individual and societal scale, the next important matter is what exactly are BCIs? BCIs are just computer systems with sensors that can measure the electrical activity inside the brain (U.S.G.A, 2016). These sensors are able to intercept and capture raw brain signals, a computer analyzes them in real time, and the signals are translated into commands. In order for you to say, lift your right arm, your brain generates an electrical signal to stimulate your right arm in some way. That signal can be detected by a sensor, and it can decipher what the signal was intending to accomplish. Right now, BCIs can only interpret motor movements, but there is an interesting aspect to this. Without stimulating the muscle, but just thinking about stimulating the muscle, modern BCIs are able to accurately interpret those same signals and translate the information encoded in those signals. To provide a concrete example, a study was performed where a person was told to simply think of a word. During this thinking process, the BCI couldn't determine what the person was thinking of. But then the person was told to imagine themselves writing down the word they were thinking of on a piece of paper. Just imagine it. And now the BCI was able to interpret the brain activity and generate the word the person was thinking of (Hart, 2021). So from these studies, it provides a good scope of where BCIs are now, and a clear path of where

they are going. Thoughts after all, are also electrical signals. So now that simpler electrical signals are being decoded, such as motor control, it may only be a matter of time before BCIs can understand and interpret other electrical signals corresponding to thoughts.

Part 3: How do BCIs relate to privacy?

Currently, BCIs lack the capacity to actually read your thoughts. However, companies like Neuralink have stated that they are working to deliver a product that is capable of "…giving them the ability to control computers and mobile devices directly with their thoughts." (Studio, 2023) And when it does, what is going to come of it? To summarize the previous part, the idea of privacy and its importance comes down to a few fundamental ideas. Privacy restricts the power that others have over you. Privacy allows for new ideas to foster and grow. Privacy enables the truest expression of oneself according to their needs and desires at any point. And privacy acts as the foundation for intimacy. The fundamental problems that BCIs pose are that it is the deepest form of continuous surveillance, which as was explained in Part 1, is what the fundamental issue is. Its not simply that BCIs can read your thoughts, its that it always is. And this consequence brings up a few questions as a result. First, is it possible to somehow build into BCIs a system of privacy? Next, is privacy even valuable in a world with BCIs? And lastly, is privacy necessary? I believe the answer to all of these questions is no.

So far, we have identified that the role of privacy is simply to protect individuals in a large number of ways. But could those same protections be realized in a society that simply doesn't have a sense of privacy?

A study performed in the US in 2019 showed that 84% of the general population firmly believes that they have little to no control over the data that the government collects (Atske, 2019). And this stands to good reason. Since the terrorist attack of 9/11, the US government has

seized the opportunity to conduct high volumes of surveillance on American citizens. Internal reports leaked from NSA confirmed that they had task forces assigned for every major smartphone manufacturer (Taitz, 2023). That alongside the fact that many mega-corporations such as Google provide user data to many government agencies around the world, the US included (Taitz, 2023). Everything from passwords, search history, payment details, and even location tracking. Social media posts have information tied to your name, where you took the photo, who else is in it, etc. How much privacy do you truly have? And how much of it do you give away willingly?

The impact of social views of privacy on technology: Where are we now?

In answering the question, how much privacy do we truly have, its important to identify what "we" even means. Here in America, 186 million people have a FaceBook account (Kemp, 2023), 150 million have TikTok (TikTok, 2023), 127 million use Instagram (Dixon, 2023), and 246 million Americans have an active YouTube account (Aslam, 2023). According to DataReportal, the average American is spending 7 hours a day, not including work hours, using a phone, computer, laptop, or tablet (Moody, 2023). Anything from scrolling through social media, streaming music, watching shows or videos, almost 1/3 of our time is spent on the internet. Leaving approximately 1/3 for sleep and 1/3 for work. This data defines who "we" refers to. To the hundreds of millions of Americans who interact with internet services for a large portion of the day.

So now it is easier to answer just how much privacy you really have. As mentioned above, these corporations that provide these internet services don't do so without asking for anything in return. By agreeing to their Terms of Service, you are allowing them to collect data and information about you. And many of us agree without a second thought. And the reason

being, its just become expected that companies are going to be collecting data on us all the time. As a society, we value what apps can provide for us more than we value the personal and private data it collects on us in return. And just how personal and private is this data? If you have ever used the internet to apply for unemployment, disability, to pay your taxes, or renew your driver's license, TikTok knows about it. And the way they know, is through Tracking Pixels. Tracking Pixels are a singular pixel on a webpage that is dedicated to sending alerts to other servers about a user's web service interaction (Ryte, 2023). Normally these are used to measure the effectiveness of an ad-campaign, however when US government websites were also found to be housing these tracking pixels, its become clear they are not only for tracking ad effectiveness, but rather collecting highly invasive personal information (Hale, 2023). Facebook alone has tracking pixels on over 13 million websites, like Cars.com, CVS, Kayak, NextDoor, and even hospital websites (BuiltWith, 2023). Advocate Aurora Health System revealed that they allow FaceBook to have Tracking Pixels on their websites that reveal sensitive health data on over 3 million patients (Minemyer, 2022). And keep in mind that this is very different from other website tracking tools such as Cookies, which you can opt out of and even delete when you're done using a websites service. Tracking Pixels are impossible to opt out of and can appear anywhere on the website. Meaning that little pop-up you get when you successfully checkout from an online store, could have a tracking pixel, letting FaceBook, TikTok, and anyone else know that you just made a purchase on a certain website. And this applies to any website. FaceBook knows when you purchase a new car, schedule a re-fill of a prescription at CVS, or even when you buy a plane ticket. It becomes much more than did you visit this website, but now even what you did on the website. And you don't even have to be using FaceBook for any of this tracking to occur. This is why I answered no to the possibility of BCIs having any form of

privacy built into their design. From our government to hospitals, everyone sees value in the collection and selling of private, personal data. With the current scale that this sort of data collection exists at, I find it entirely unreasonable to believe that any company that does end up producing a marketable BCI will stray from this industry standard.

The impact of social views of privacy on technology: How did we get here?

In the previous section, I analyzed the corporate commercialization of individual privacy in America. I now want to shift the focus towards a social perspective, and I will now analyze how we got to this point where this is the status quo of modern living. How did this start? It started with the social commercialization of individual privacy.

Privacy-Invasion as Entertainment

Right around the 1990s, shows featuring hyper-invasive surveillance became some of the biggest hits on Television. The viral sensation of Nasubi in the late 90s is a perfect example. Nasubi is the name of a Japanese contestant on one its darkest Japanese reality TV shows. The show was to have someone survive for as long as they could in one small room, only able to use what they win in sweepstakes. Starting off with nothing, no food, no clothes, no connection to the outside world, it was just him and a studio camera recording him 24/7. Every Sunday of the week, the producers would essentially make a highlight reel of what they thought was the most entertaining parts of the week. And every Sunday night, 17 million people in Japan tuned in to watch, captivated by the show (Hamatsu, 2015). It was so popular it became the single highest rated show in Japan, breaking numerous records in regard to viewership. And this is just the beginning. The entertainment of invading the privacy of others proved to only skyrocket. Shows like Hoarders, Big Brother, and The Real World are all examples of this evolving interest in total

privacy invasion. The idea of being able to spy on people is simply a captivating and appealing concept, explaining the wild success of many of these shows.

And while all this is happening, a new social paradigm is beginning. Prior to the widespread use of the cellphone, if you made plans to go out and do something, no one could reach you for the entire time you were gone until you returned home to check on your emails or voicemails. But in the age of mobile smart phones and social media, its almost expected that if you are going somewhere, you make a post about it. You tell the world about your life anytime something of interest happens. You're going on a vacation; you make a big post about all the things you did. You ended up in a hospital; you make a big post of you in the hospital bed. The idea that you could see into the lives of others, even if it was just a glimpse or snapshot, absolutely exploded. And this has brought us to where we are now, where socially, it is very prevalent that internet fame and notoriety is something to desperately sought after, and there are many people who are willing to do anything for fame. Whether it be exposing some of their lowest points in dramatic breakups to intentionally sabotaging relationships to build drama, what was once considered to be some of the most private portions of your life were now publicly viewable by anyone at any time. And still, it didn't stop there. Now instead of just recording your own life for the sake of entertainment with the development of YouTube families, where the entire basis of their content is to record every aspect of their families' waking lives, it has extended into recording other people in this same highly invasive nature. The content of YouTube families tends to be supercuts, or big montages of whatever will get the most views, often being huge celebrations, or heart-breaking news and drama. It has become normal for these people to record themselves and make public some of their lowest points in life. I believe it is

within this new social paradigm that my answer to the question of if privacy is valuable is justified. As in fact, the exact opposite of privacy is what is valued. It is incredibly valued to always put your life in the spotlight, no matter what it may reveal, so long as you can maintain a social status of popularity and approval. A theme that is remarkably reminiscent of fictional works like Black Mirror's Nosedive episode. In this world, it has made the transition from high ratings being a highly desirable component of a higher social status, to being the foundation of who is considered to be worthy of benefiting from society. And this artistic exaggeration of society emphasizes the fact that privacy is a fleeting concern. What people value now is essentially their social rating and are willing to do just about anything to increase it.

The impact of social views of privacy on technology: Do BCIs change anything?

Now returning back to the focus of this piece, being the social impact of the privacy invasion of BCIs, I think it stands to reason those 14 protections of privacy outlined in the introduction, are already undermined at an almost unfathomable scale. Unless you live off the grid, the reality is you almost don't have privacy at all. Almost anything you do to interact with the modern world is monitored and tracked. So, the question is do BCIs undermine our privacy substantially more. And I believe the answer is no. The reason must deal with the matter of consciousness and our awareness of it.

How much of our thoughts do we control?

To understand if having access to our thoughts is meaningful, the term "our thoughts" should be defined. When I am referring to thoughts, I am specifically referring to thoughts that we are consciously aware of and inherently have control over. According to many cognitive neuroscientists, we are only consciously aware of about 5% of our cognitive activity. Which

means the remaining 95% of our decision making, actions, emotions, and behavior go completely beyond our conscious awareness (Szegedy-Maszak, 2023). Many of our decisions are made or strongly influenced by what is coined the Adaptive Unconscious. The adaptive unconscious is a learning scheme our brains have developed that produces efficient information processing, filtering, judgement, and even creates goals for you to unconsciously pursue (IResearch, 2022). A remarkable percentage of our lives are essentially driven by this adaptive unconscious, and this produces a vast majority of the observable and intimately monitored behaviors that have been outlined through this paper. So to have a machine that can potentially view the remaining 5% of our cognitive activity seems unimpactful, as only 5% of our behavior is actually controlled by us consciously.

Part 4: The Conclusion

A brief overview of the topics discussed so far is first, an analysis of why privacy is an important matter, followed by a brief introduction to the technology of BCIs and their associated problems with privacy. Then a discussion on the current state of privacy in the modern world without BCIs, leading to an analysis of one component of how this came to be, and lastly discussing how much BCIs could deepen the issue. It has been discussed that the modern world features such an overwhelming degree of surveillance and monitoring, that virtually any way of interacting with modern society over the internet is contributing to detailing and refinement of your data profile that is shared among numerous mega-corporations. It has then been shown how we as a society sort of took the first steps into popularizing this from a conceptual standpoint, and how we have shifted our paradigm into one that finds this completely normal, and without second thought routinely encourages it. And in the end, a neuroscientific approach demonstrated that the data that is collected regarding our outward and expressive behavior is extremely

correspondent with who we are, and the information capable of being extracted from that alone is enough to almost have a formulaic synthesis of who we are, the additional information that could be gathered through BCIs would aid in completing this data profile, its far from contributing substantial additional information. Because of this, I believe that the incorporation of BCIs into society would not have a substantial impact on the undermining of individual privacy.

Bibliography:

Administrator, "Adaptive unconscious (Social Psychology)," Psychology,
        http://psychology.iresearchnet.com/social-psychology/control/adaptive-unconscious/

C. Hale, "TikTok trackers found on multiple US government websites," TechRadar,
        https://www.techradar.com/news/tiktok-trackers-found-on-multiple-us-government-
        websites

D. J. Solove, *A Taxonomy of Privacy*. University of Pennsylvania.

M. Hart, "Brain-computer interface turns mental writing into text," Nerdist,
        https://nerdist.com/article/brain-computer-interface-turns-mental-writing-into-text/

M. Szegedy-Maszak, "Mysteries of the Mind," Mysteries of the mind,
        http://webhome.auburn.edu/~mitrege/ENGL2210/USNWR-mind.html

Nasubi, Wikipedia, https://en.wikipedia.org/wiki/Nasubi

P. Minemyer, "HHS bulletin clarifies when pixel tracker use may violate HIPAA," Fierce
        Healthcare, https://www.fiercehealthcare.com/health-tech/hhs-bulletin-offers-clarity-when-
        use-pixel-trackers-may-violate-hipaa

P. Studio, "Applications," Neuralink, https://neuralink.com/applications

R. Moody, "Screen Time Statistics: Average in the US vs. rest of the world," Comparitech,
        https://www.comparitech.com/tv-streaming/screen-time-statistics/

S. Atske, "Americans and privacy: Concerned, confused and feeling lack of control over their
        personal information," Pew Research Center: Internet, Science & Tech,
        https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-
        confused-and-feeling-lack-of-control-over-their-personal-information/

S. Dixon and F. 15, "Number of U.S. instagram users 2023," Statista,
        https://www.statista.com/statistics/293771/number-of-us-instagram-users/

S. Kemp, "The latest Facebook statistics: Everything you need to know - datareportal – global
        digital insights," DataReportal, https://datareportal.com/essential-facebook-stats

S. Taitz, "Five things to know about NSA mass surveillance and the coming fight in Congress:
        ACLU," American Civil Liberties Union, https://www.aclu.org/news/national-
        security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-
        congress.

TikTok, "Celebrating our thriving community of 150 million Americans," Newsroom, https://newsroom.tiktok.com/en-us/150-m-us-users

T. J. Magi, *Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature*, vol. 81. The University of Chicago Press, 2011.

"Tracking pixel," What are Tracking Pixels and How Do They Work?, https://en.ryte.com/wiki/Tracking_Pixel

U. S. G. A. Office, "Science & Tech spotlight: Brain-Computer interfaces," Science & Tech Spotlight: Brain-Computer Interfaces | U.S. GAO, https://www.gao.gov/products/gao-22-106118

"Websites using Facebook Pixel," Websites using Facebook pixel including historical, https://trends.builtwith.com/websitelist/Facebook-Pixel/Historical

"YouTube by the numbers (2023): Stats, Demographics & Fun Facts," Omnicore Agency, https://www.omnicoreagency.com/youtube-statistics/