 [1]

Privacy and Brain-Computer Interfaces
Dept. of CS, University of Victoria
April 2017

Abstract

Brain Computer Interfaces (BCIs) have gained popularity in recent years as these systems can control a variety of external machines such as cursors on monitors, televisions, wheelchairs, robotic arms and have assisted many with disabilities in their daily lives. Although this sounds promising, the nature of this technology, which allows others to make inferences about our memories, intentions and conscious, or unconscious interests using accessible brain wave patterns, raises some concerns around the exploitation or mishandling of BCIs devices. Thus, the goal of this paper is to start a discussion about possible steps to mitigate these emerging issues.

- ECoG = Electrocorticography
- ICE = Intracortical electrodes
- fNIRS = Functional near-infrared spectroscopy
- fMRI = Functional magnetic resonance imaging
- EEG = Electroencephalography
- MEG = Magnetoencephalography
- ERP = Event Related Potential
- BCI = Brain Computer Interface
- HIPPA = Health Insurance Portability and Accountability Act

Introduction

Have you ever imagined a world where you can manipulate machines via thought? While this may sound like a glimpse of the far future, implementation of this notion is more contemporary than one could expect. Brain-Computer Interfaces (BCIs) or brain-machine interfaces are a modern new means of interfacing with computers and other devices. While the definition of a "pure BCI" has many variations, the most recent cited description states that: Brain-computer interfaces (BCIs) enable non-verbal communication between users and devices by using the measured brain signals for communication (Takabi). In short, BCIs facilitate direct communication between a brain and an external device such as a computer or smart phone. In the past, BCIs have mostly been used in medical fields to assist in recovering human cognitive capabilities. However, in recent years, researchers in laboratories around the world realized the capabilities of these systems and started using BCIs in fiction, gaming, marketing and the entertainment industry. In fact, BCIs interpreting electroencephalographic (EEG) data, which refers to tests that detect brain activity using flat metal discs, can be purchased online at very low costs e.g. Emotiv Systems, NeuroSky, MinSolutions, Muse and IntendiX (Wahlstrom, Fairweather, Ashman). Therefore, this paper will identify the different types of BCIs, some of the current applications of BCIs and how they operate, as well as the arising ethical implications and potential privacy disruptions from using such innovation. Emphasis on privacy issues and threats will take place from both a security and social contexts by considering different privacy theories and relating them to BCIs. Then, recommendations will be made to possible countermeasures that can be taken.

Device	Price	Electrodes	Resolution	Interface
BioSemi Active [3]	$12000	256	24 bits	Wired
Emotiv EPOC [4]	$399-499	14	14 bits	Wireless
NeuroSky [5]	**$50-150**	1	8 bits	Wireless

Table 1: BCI Devices (Li, Ding, Conti)

Current BCIs Applications

There are three types of BCIs in terms of invasiveness: invasive, partially invasive and non-invasive. The first one is directly implanted into the brain during surgery, which can measure the highest quality of brain signals. Although this type has deeply targeted monkeys and rats, it has been tested on only a few severely disabled people due to body complications that could surface with new objects implanted. The second type of BCIs is implanted inside the skull on top of the brain, and the third type involves using external electrodes which is the most frequently used one due to the fact that it can easily use electrical signals produced by neural brain activities (Bonaci, Chizeck). Neuromarketing is one example of an application that has been an interest for BCI researchers. Companies such as Google and CBS TV have used neuromarketing services because it is claimed to be the most recent mechanical method used to understand consumers (Kolter, Burton, Deans, Brown & Armstrong). Using MRI and Electroencephalography (EEG) scans; researchers and marketers gain a greater understanding of human's cognition and behavior in response to products and advertisements stimuli. This has established valuable theoretical insights, which enabled business vendors to gain insight into consumers' intentions and emotions towards branding and market approaches (Shiv & Yoon). Moreover, in the medical field, BCIs are used to treat children with Autism Spectrum Disorder (ASD), e.g. Figure 1 shows that the user's EEG and peripheral physiological measures are recorded and used in the Social Mirroring Game, which gives the user visual feedback. For positive feedback (in green), the child's avatar must first approach the non-player character and has to exhibit some brain activity by imitating the facial emotions of the non-player. Negative feedback (in red), involves the child's avatar being not responsive to the non-player. The game helps children learn how to change their brain activity and have some control over the game (Friedrich, Suttie, Sivanathan, Lim, Louchart, Pineda).

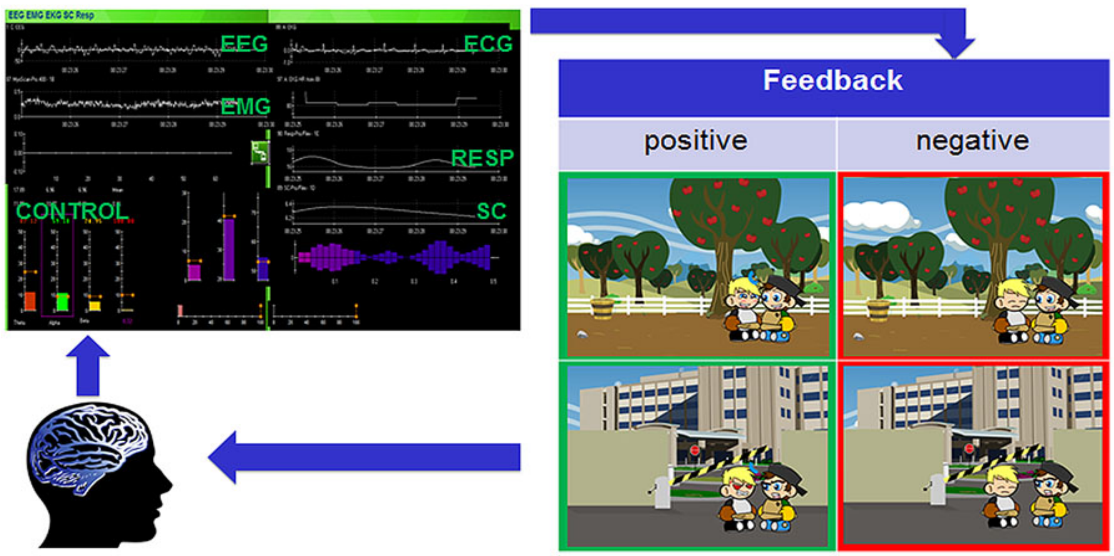

Figure 1: BCI in Social Mirroring Game (Friedrich, Suttie, Sivanathan, Lim, Louchart, Pineda).

BCIs Mechanics

BCI is a communication system consisting of inputs as user's neural activity, outputs as external commands and components to handle inputs and outputs known as *signal acquisition* and *signal processing*. Signal acquisition comprises of the hardware that measures brain signals and signal processing is the software that extracts the necessary information (Bonaci, Calo, Chizeck). Commands pass through the next two stages before they can be transferred to a machine.

Signal Acquisition

First, BCI devices capture brain analog neural signals using one of the following methods:

- Electrocorticography (ECoG)
- Intracortical electrodes (ICE)
- Functional near-infrared spectroscopy (fNIRS)
- Functional magnetic resonance imaging (fMRI)
- Electroencephalography (EEG)
- Magnetoencephalography (MEG)

EEG-based devices are the most widely used and can capture up to five different waves from human brain activities as follows: 1) Gamma wives associated with arousal and excitement 2) Beta waves related with action and concentration 3) Alpha waves related with relaxation 4) Theta waves associated with daydreaming and inefficiency 5) Delta waves related to hypnosis (Li, Ding, Conti).

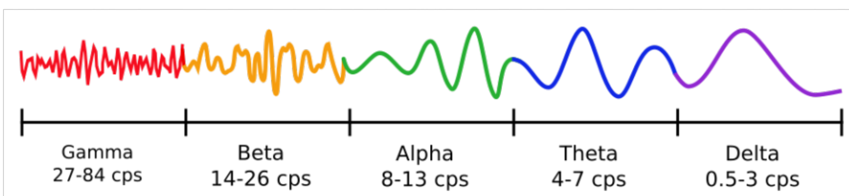

Figure 2: Brain Waves (http://elearningwiki.com/index.php?title=PhysicalBrain)

Signal Processing

Analog signals are then translated into digital signals and go through two processes: ***feature extraction*** to amplify and filter out noise and ***translation algorithm*** to determine the user's general brain pattern, and predict some aspect of the person's cognitive state, attention or intention. (Bonaci, Calo, Chizeck).

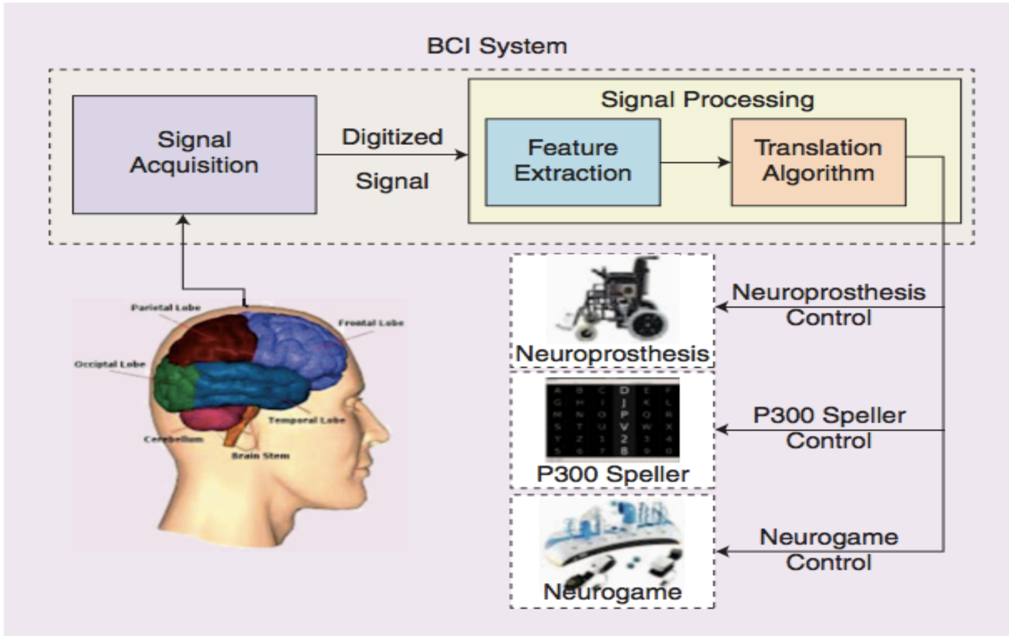

Figure 3: How BCI system works (Bonaci, Calo, Chizeck)

BCI Typology

This section's proposition is from the contextual theory of information privacy, which states that "privacy and social context are inter-related and disruptions to social context may disrupt privacy" (Nissenbaum). Thus, prior to attempt to identify privacy issues, the typology of BCIs will be identified first with consideration of user's context. BCI research direction has classified BCIs broadly according to whether the technology is invasive, partially invasive or non-invasive. Other attempts of classification relied on signal type such as *spontaneous signals*, which are produced deliberately by the user, and *evoked signals*, which are caused by recognition of a stimulus unintentionally (Wahlstrom, Fairweather, Ashman). In a similar approach, Zadner et al. uses a different terminology, referring to spontaneous and evoked signals as active and reactive, respectively as well as adding a third type, passive BCIs where neural signals are involuntary acquired and analyzed. Here in this paper, four types of BCIs will be reviewed and to indicate the maturity of each type, three subcategories will be introduced.

1- Active BCI

As described before, active BCI collects neural signals produced intentionally by the user. For instance, the user may manipulate a pointer on a computer monitor by extending their index finger (Wahlstrom, Fairweather, Ashman).

- **Existing**: A study was conducted in 1991 to train individuals with severe motor deficits to use brain activity to move a cursor from the center of a computer screen to the bottom of a page (Forneris, Neat, McFarland, Wolpaw).
- **Prospective**: In 2009, a group of researchers investigated the interaction between BCI and a machine that needed precise timed control tasks such as pinball. It was concluded that a well-timed and fast control is very possible even within an environment rich with visual and auditory distraction (Vidaurre, Blankertz, Muller)
- **Speculative**: The possibility to use an active BCI with a mathematical game to curtail anxiety has been under research (Wahlstrom, Fairweather, Ashman).

2- Reactive BCI

Reactive BCI derives its output in reaction to external stimulation. For example, when a user becomes familiar with an image and then a series of images is displayed rapidly on a computer monitor, the user recognizes the first image and in response to this cognitive event, he/she exhibits a feature called Event-Related Potential (ERP) (Wahlstrom, Fairweather, Ashman).

- **Existing**: Early in 1990, ERP was used to aid individuals who cannot use any motor system for communication e.g. locked-in patients (Farwell, Donchin)
- **Prospective**: In more recent years, advances in motion detection technology have made it easier to assess human movement instantaneously and with high accuracy, using small sized vibrotactile actuators (device to produce haptic feedback). This aids users on how and when to

move their arm for instance by providing immediate feedback (Bark, Hyman, Tan, Cha, Jax, Buxbaum, Kuchenbecker)

- **Speculative**: Currently, BCIs technologies lack robustness due to two factors: 1) individual variability in neural signals and 2) intraindivudal differences over time. Thus, it is still unknown how these variabilities affect BCI performance. However, BCI paradigms have been recently embedded in games with a purpose (GWAP) to assist in solving research questions. (GWAP is a method of delegating a computational process to humans in an entertaining way) (Lance, Touryan, Wang, Lu, Chun, Chuang, Khooshabeh, Sajda, marathe, Jung, Lin, Mcdowell).

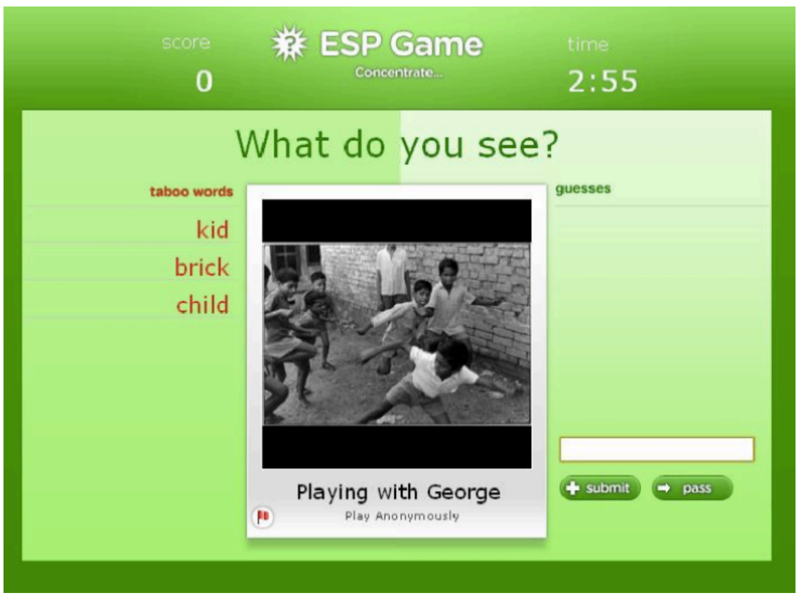

Figure 4: GWAP ***(http://www.iis.sinica.edu.tw/~swc/pub/social_verification_model.html)***

3- Passive BCI

Passive BCIs implicitly gain information from user's brain activity without the need for the user to control his/her brain activity. E.g. when a user is engaged in a complex task and is concentrated, neural signals can be acquired and analyzed (Wahlstrom, Fairweather, Ashman).

- **Existing**:

Application	Task	Brain features	Goal	Usage of implicit interaction
Video games	Game (Bacteria Hunt)	Alpha band power	Challenge player to relax	Affect controllability of avatar
	Game (AlphaWow)	Alpha band power	Enhance immersion	Shift avatar's form
	Game (Tetris)	Blood oxygenation (fNIRS)	Enhance immersion	Adapt music to the predicted user's task
	Game (RLR)	Errp	Detect user's feeling of losing control	Detect if the user perceived a system's error

Table 2: Passive BCIs in video games (George, Inria, Bunraku)

- **Prospective**: EEG data has been able to detect covert attentiveness; a situation when a user's behavior shows their attention is involved in a certain task, when in fact it is engaged somewhere else.
- **Speculative**: A specific framework using passive BCI has been proposed in 2015 to measure users' reactions to a system's interface immediately instead of using psychological metrics.

4- Hybrid BCI

Hybrid BCI can be more reliable as they can improve performance and functionality by means of acquisition and analysis (Wahlstrom, Fairweather, Ashman).

- **Existing**: In 2004, an active BCI and a finite state automaton (machine that can be in exactly one of a finite number of states at any given time) were combined to allow the continuous control of a mobile robot. The goal was to move the robot through different rooms in a house-like environment. Thus, eight surface electrodes were used and the interface was made to work asynchronously, so the person was able to make self-paced decisions on when to switch from one mental task to another.

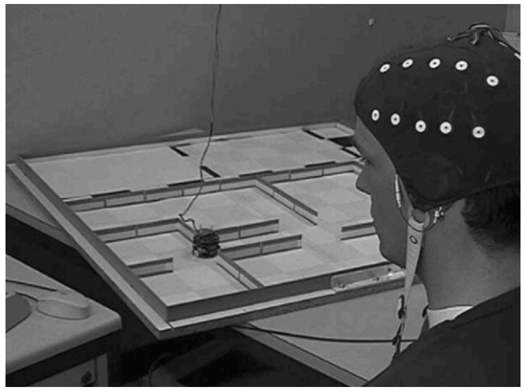

Figure 5: A participant trying to move the robot with his thoughts

(Millan, Renkens, Mourino, Gerstner)

- **Prospective**: In 2011, electroencephalographic (EEG) and electromyographic (EMG) were parallelly used to help disabled people with residual activity of their muscles. Users achieved a good control of their hybrid BCI in spite of their muscular fatigue (Leeb, Sagha, Chavarriaga, Millan)
- **Speculative**: Active BCI was combined with functional electrical stimulation (FES) in 2015 to improve hand function in participants with tetraplegia (paralysis caused by illness or injury). FES refers to a technique that utilizes low energy electrical pulses to artificially generate muscle contractions and body movement. (Vuckovic, Leslie, Allan, B.Frcs)

Privacy From a Social Context

Privacy has been around for some time now, and it has taken different shapes and forms. Although not mentioned explicitly, Section 8 of the Canadian Charter of Rights and Freedoms states "Everyone has the right to be secure against unreasonable search or seizure". Alternatively, privacy is a basic right necessary for human dignity as established in the Universal Declaration of Human Rights. However, emerging technologies such as BCI have challenged our perception of what privacy is. Therefore, five privacy theories will be discussed here and BCI technologies will also be considered with respect to these theories in order to identify any privacy issues.

1- Control Theory

In here, privacy refers to the ability to control one's personal information i.e. how, when and how much can be exposed to others (Wahlstrom, Fairweather, Ashman).

- **Active BCIs**: Two situations here: 1) users must use BCI to engage in everyday life activities e.g. a disabled person who wants to have a private phone conversation using a vocal synthesizer. In this case, it is important to control privacy. 2) User is not obligated to use BCI, yet engage intentionally in tasks involving BCI. In this case, if the user has provided consent for the acquisition of their neural information, then active BCIs do not pose any privacy issues.
- **Reactive BCIs**: Since event-related potential (ERP) is used in this technology, there is a potential privacy issue especially if the user is forced into using a Reactive BCI such as in police interrogations. In this case, the user may generate ERP signal in response to a particular stimulus that he/she would not prefer to share. Otherwise, if a meaningful consent is given then privacy issues are unlikely to arise.

- **Passive BCIs**: Since users do not control passive BCI and users are performing complex tasks such as a pilot manipulating plane controls. In this case, a privacy issue may arise under the control theory because users are engaged in a demanding task in uncontrolled environment and it might be difficult to disengage from using BCI before signals are taken.
- **Hybrid BCIs**: The potential privacy issues arising from hybrid BCIs are similar to those arising from active, reactive or passive.

2- Restricted Access Theory

The main idea here is that privacy is comprised of restricted access to persons or information about persons. Thus, a person or a group has privacy in a situation if and only if the person or group or information related to the person or group is protected from intrusion, observation and surveillance by others. This necessitates a requirement for regulatory frameworks (Moor). Thus, if data obtained by BCIs is protected under some regulatory frameworks then direct control over personal information is possible and privacy is not disrupted. This is inferred from the fact that personal information can proliferate once it is disclosed (Wahlstrom, Fairweather, Ashman).

3- Privacy As A Commodity Theory

There has been some debate over the meaning of privacy as a commodity. Some suggests that the right to privacy comes from other rights such as the right to ownership of property. While others argue, "that the rights from which the right to privacy derives can be as readily conceived as derived from the right to privacy." However, these notions did not prevent privacy issues from arising while incentives to collect personal information have been enough to disrupt privacy. Thus, current definition of privacy as commodity entails that if personal information is shared in a market, privacy is disrupted. This means that the ownership of data obtained by BCI should be set up prior to the usage of BCI. Privacy becomes an issue if someone acquires a copy of BCI data without purchasing it from its owner. (Wahlstrom, Fairweather, Ashman).

4- Contextual Theory

This refers to how cultural and social factors can influence a person's idea of privacy and its relation to social norms arising from interests such as dignity, autonomy and reputation, i.e. if information flow disrupts the established integrity of a context, then privacy issues are likely to arise. (Wahlstrom, Fairweather, Ashman).

- **Active BCIs**: The norm here is opting out or in. If a user is voluntarily engaged in the usage of BCI and has given consent for the collection of their data, then there would be no issues in this case as circumstances are consistent with the norms. However, if a user is compelled to use BCI due to conditions beyond their control such as disabled people, then privacy disruption may occur.
- **Reactive BCIs**: Obtaining a meaningful consent is the norm here. However, privacy disruptions depend on existing social norms, so if, for example, interrogation technologies do not permit collection of ERP signals then reactive BCIs may raise some privacy issues here, although sometimes a privacy disruption becomes socially acceptable when it serves for the best of the community.
- **Passive BCIs**: Since this involves uncontrolled environment and complex tasks, privacy issues are raised if social norms are disrupted e.g. retraction of consent while doing cognitively demanding tasks.
- **Hybrid BCIs**: The potential privacy issues arising from hybrid BCIs are similar to those arising from active, reactive or passive.

5- Ontological Theory

Here, personal information is constitutive, i.e.

"One may still argue that an agent "owns" his or her information, yet no longer in a vaguely metaphorical sense, but in the precise sense in which an agent is her or his information. "My" in "my information" is not the same "my" as in "my car" but rather the same "my" as in "my body" or "my feelings": it expresses a sense of constitutive and intimate belonging, not of external and detachable ownership, a sense in which my body, my feelings and my information are part of me but are not my (legal) possessions" (Floridi).

Thus, in respect to BCI, the highly constitutive the neural data, the greater the chance of privacy issues arising. (Wahlstrom, Fairweather, Ashman).

	Active	**Reactive**	**Passive**	**Hybrid**
Control Theory	C1	A, C2	A	A
Restricted access	A	A	A	A
Commodification	A	A	A	A
Contextual	C1	A, C2	A	A
Ontological	A	A	A	A

Table 3: Summary of privacy disruptions (Wahlstrom, Fairweather, Ashman).

C1: potential privacy disruptions arising for users who are compelled to use a BCI

C2: users who are coerced to use a BCI

A: denotes all users

Ethical and Legal implications

BCIs systems integrate many disciplines such as “biomedical engineering, neuroscience, computer science, electrical and computer engineering, materials science, nanotechnology, neurology and neurosurgery” (Berger). With the increasing number of BCI applications and the emergence of non-medical areas, researchers have recognized the need to introduce neuroethics. For instance, brain fingerprinting is a controversial unproven technique to determine hidden information in one's brain in order to find the truth. Regardless of how questionable this is, the collection of brain data is similar to that of genetics in that behaviors are likely to be detected, and both types of data can expose personal and uncontrolled aspects of a person. William Safire, a journalist and ethicist has displayed his concerns around neuroprivacy and has commented:

"The specific ethics of brain science hits home as research on no other organ does. It deals with our consciousness—our sense of self—and as such is central to our being. What distinguishes us from each other beyond our looks? The answer: our personalities and behavior. And these are the characteristics that brain science will soon be able to change in significant ways. Let’s face it: one person’s liver is pretty much like another’s. Our brains, by contrast, give us our intelligence, integrity, curiosity, compassion, and—here’s the most mysterious one— conscience. The brain is the organ of individuality." (The committee on Science and Law)

Because of this, the Committee on Science and Law proposed in 2005 for neuroethics to take on similar ethical and legal rules already set forth in genetic research (Bonaci, Calo, Chizeck). However, predicting future behavior sometimes is necessary to protect society from a dangerous conduct such as sexual predators, abusers and other criminals. Therefore, genetic laws may not be useful and new laws may be necessary to develop for these situations, as the legislature should take into account the individual privacy against the police power.

Privacy From a Security Perspective

BCI is a recent technology and expanding relatively fast in different areas ranging from education, entertainment, gaming … etc. Because of this, manufacturers promote open-development platforms to enhance the technology. However, this can compromise user's privacy by giving developers full control over BCI components discussed before (Signal processing system and translation algorithm). For instance, a software known as "Brain spyware" was the first malicious BCI application born in 2012. It was tested on users where they were presented with visual stimuli and their ERP P300 signals were captured. This data could be analyzed and help reveal user's info such as pin#, bank information, birthdate, location, memories, prejudices, beliefs and possible neurophysiological disorders. A more serious threat was identified later in which the BCI victim is targeted at levels below his/her cognitive perception and exposed to visual stimuli for 13.3 milliseconds. This is known as subliminal attack and was shown to be effective for extracting personal data. Unfortunately, there are no current regulations that prevent the collection of such data outside of medical privacy and security rules (HIPPA in the US), and the impact of exploiting user's brain signals is difficult and may be severe if not addressed early on. (Bonaci, Calo, Chizeck). However, prior to dive into more security issues and countermeasures, authors Bonaci and Chizeck advise answering the following questions:

- Who should have an access to an individual's neural information?
- Which components of the neural information should those entities have an access to?
- How noisy, distorted or distilled should these components be made before making them available?

- Which purposes are the entities allowed to use the brain signals for?
- Are the entities allowed to present individuals with new stimuli, or extract new signal components or components thereof, to make inferences about an individual?

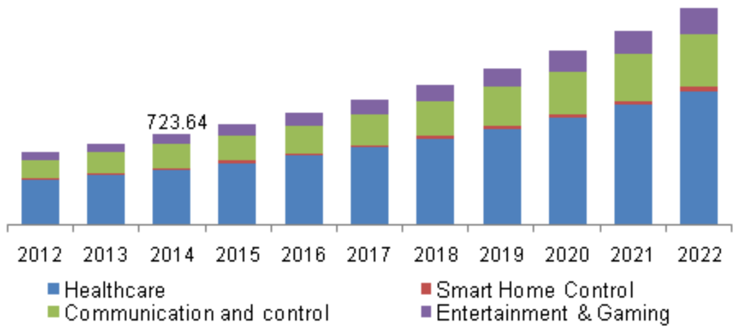

Figure 6: BCI Market *(www.grandviewresearch.com/industry-analysis/brain-computer-interfaces-market)*

Privacy Scenarios and Countermeasures

Four ways private data can be compromised will be covered next and the possible ways to prevent them:

1- Neuromedical Applications

Attacker can control patients' implant devices such as prosthetic limbs via intercepting the transmission of wireless brain neural signals between a BCI device and physician's application. The main thing here is to protect the patient from life-threating attacks as well as leakage of personal information, e.g. an attacker could decompose raw wireless signals to manipulate a patient and give dangerous movements. There are no current robust safeguards to prevent these types of attack (Li, Ding, Conti).

2- User Authentication

Adversaries can impersonate thoughts of the subject to authenticate themselves e.g. finger movement, breathing, smiling or singing. Also, an attacker can compromise an authentication system via using synthetic EEG signals, which he/she can obtain from historical EEG data of the victim. One possible way to curtail authentication attacks is to mitigate authentication error rate. Another method is by using multiple authentication signal factors e.g. breathing and being shocked signals are combined together to perform multidimensional authentication (Li, Ding, Conti). Takabi in his paper "Firewall for Brain" proposes a solution based on BCI applications and the tasks they perform on brain waves rather than using general-purpose privacy preserving technologies. The approach called "MindShield" and is composed of different layers of privacy protection.

- One layer uses *homomorphic encryption* and *functional encryption*. Homomorphic encryption is a type of encryption that allows computations to be executed on the cipher text, while functional encryption is a generalization of public-key encryption in which possessing a secret key allows one to learn a function of what the cipher text is encrypting. (Huang, Zhou).
- Another layer uses access controls to limit application's access to brain waves.
- An extra component is used to analyze whether the BCI application presents any stimuli in a legitimate way.

3- Gaming and Entertainment

BCI games utilize third party APIs to use BCI devices. These APIs provide unrestricted access to raw brain activity signals, which allows attackers to design games and videos that take advantage of this vulnerability, e.g. P300-Speller is a game that has characters arranged in a matrix of rows and column. These flash rapidly on a screen while the user focus on one character each time using their eyes until they get the word they want. These types of attacks called side-channel attack and can be prevented using "BCI Anonymizer". This works by removing private information from raw EEG signals except for specific intended BCI commands. Removed signals that represent private data can be replaced by anonymized generated neural signals. BCI can be embedded in either BCI's hardware or software but never in any external network. This way, "BCI Anonymizer" ensures security by providing BCI device with only needed data (Li, Ding, Conti).

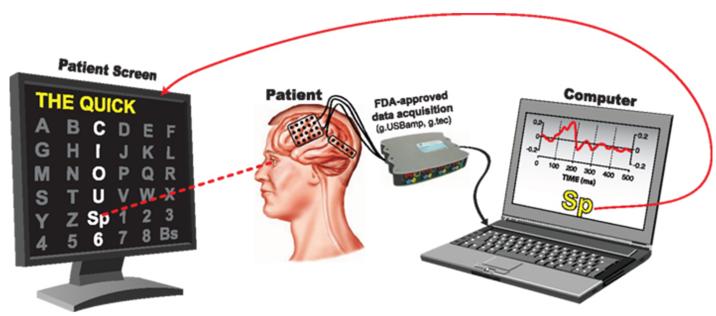

Figure 7: P300-Speller Game *(http://journal.frontiersin.org/article/10.3389/fnins.2011.00005/full)*

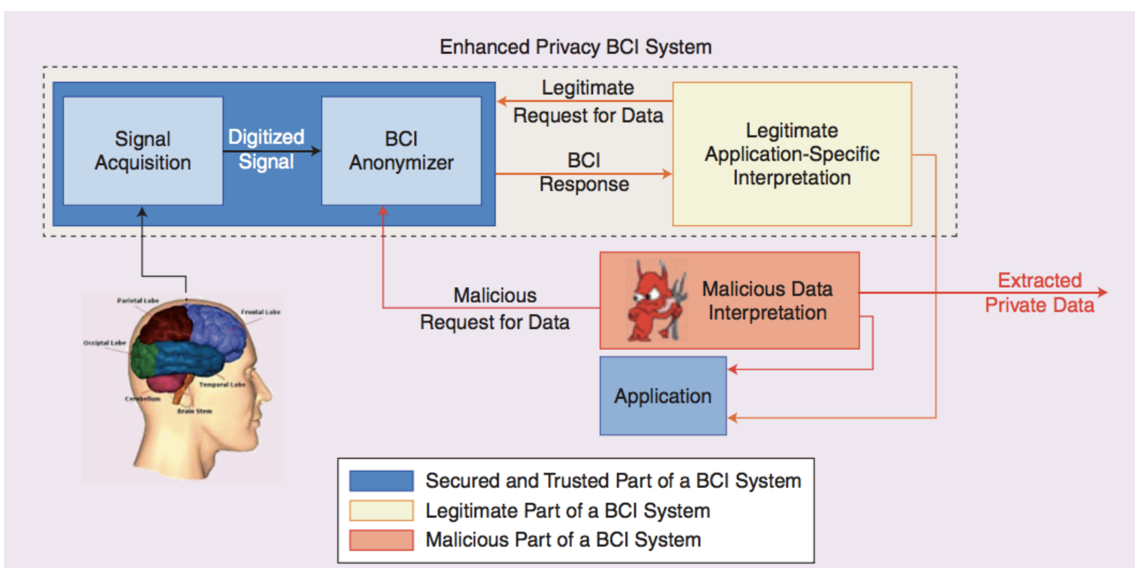

Figure 8: Anonymizer Subsystem (Bonaci, Calo, Chizeck)

4- Smartphone-based Applications

Possible attacks here are similar to that of smartphones. Since data is often stored in the phone or SD card, it becomes easily infected with malware, e.g. a brain-controlled address book dialing app works in the same way as the P300-Speller discussed before where the user is shown a series of photos of contacts that he/she wishes to call. Levels of attention and meditation can be recorded and saved on the phone, which could jeopardize the patient's privacy later on. Since this is a smartphone-based application, security measures followed in smartphones can also be applied to BCI applications e.g. TaintDroid is a real-time monitoring service that is installed at a low level of the Android system in order to track how apps access and use sensitive information (Li, Ding, Conti).

Opposing Views

Similar to every other technology, BCIs have their own advantages and disadvantages. Invasive methods such as probing electronic equipment into humans' organs have its own risks. Using electrical electrodes on skin can cause itching, pain or discomfort to the wearer. Even worse, mind reading makes a terrifying reality. However, this paranoia might be exaggerated and could be influenced by inaccurate and fictional portrayals. Martinovic in his paper "On the Feasibility of SideChannel Attacks with Brain-Computer Interfaces" claims that brain hackers do not have much information to attain at any given time. Figure 8 shows a general brain activity reading, which is the only thing an attacker, can utilize. Yet, this increases the attacker's chance of interpreting this information by only 5-20%. This, however, does not disapprove or undermine potential threats. Sophisticated attacks are possible and can be achieved depending on the attacker's creativity. Therefore, uninformed users could be easily manipulated and engaged into mind games.

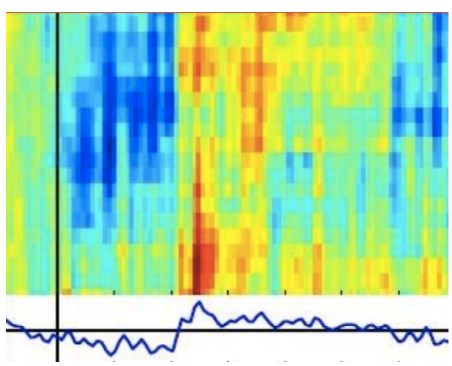

Figure 9: User's General Neural Activity (Martinovic)

Conclusion

Although that BCI technology is on the rise, it is considered fairly limited to research and medical communities. In fact, this is advantageous because it gives us time to reflect on current privacy issues and technical challenges such as those covered in this paper before they manifest in the future. Thankfully, BCI research is ongoing despite the shortcomings such as the lack of processing power needed to process huge amount of neural signals in real time, or the reliance on user's input to preserve privacy (Takabi). The potential that BCI innovation will enhance the human condition is only limited by our minds, and in order to support the dissemination and usage of BCI by consumers, very much attention needs to be given first to privacy. Thus, effort in this paper (although limited and some analysis may have been overlooked) was made to investigate initial and existing research steps towards facilitating the needed interdisplinary discussion and beginning to design privacy-preserving and secure BCI systems. The second important thing is that legal protection of neuroprivacy is required as there are no current laws and provisions to protect such data. As mentioned before, the committee on Science and Law suggests using genetic privacy legislation as a starting model for shielding against some of the concerns that could arise from BCI technology. This is because brain information is just like genetic information in the way both have the potential to yield great benefits or great dangers. In the 1970s, employers used tests developed to screen for the presence of sickle cell anemia, which mostly affected African-American at the time. Some of these tests were done without the employee's knowledge, which resulted in discrimination and lack of privacy until the National Sickle Cell Anemia Control Act was passed in 1972. Therefore, the fears expressed in respect to genetics are similar to those concerns expressed with respect to neuroprivacy. Donald Kennedy, a neurobiologist and editor in Science says:

*"I already don't want my employer or my insurance company to know my genome. As to my brainome, I don't want anyone to know it for any purpose whatsoever. It is . . . my most intimate identity" (*The committee on Science and Law).

However, although both genetic and brain information share a lot in common, they differ in what they can predict. Genetic information are mainly used to predict future diseases while brain information is aimed at predicting future behavior which has more privacy implications than that of genetics. Another difference is that genetic privacy protection laws do not protect against recording peoples' thoughts in real time, which makes it a less useful model for protection. Furthermore, brain processes are arguably controlled by many factors more than genetics, e.g. obtaining brain data requires one's conscious participation while in a genetic test, one's participation is minimal. This makes interpretation and analysis of information more complicated in a brain imaging, for instance. Therefore, based on the discussion above, it seems adopting the genetic privacy protection as a model to address neuro privacy concerns, would be a great start in spite of its limitations (The committee on Science and Law).

Works Cited

L.A. Farwell, E. Donchin. "Talking off the top of your head: toward a mental prosthesis utilizing event-related brain potentials ☆ ." Dec 1988. ScienceDirect. <http://www.sciencedirect.com.ezproxy.library.uvic.ca/science/article/pii/0013469488901496>.
Vuckovic, Aleksandra PhD, Leslie OT Wallace and David B. FRCS Allan. "Hybrid Brain-Computer Interface and Functional Electrical Stimulation for Sensorimotor Training in Participants With Tetraplegia: A Proof-of-Concept Study ." Jan 2015. Ovid.
Brent J. Lance, Jon Touryan, Yu-Kai Wang, Shao-Wei Lu, Chun-Hsiang Chuang, Peter Khooshabeh, Paul Sajda, Amar Marathe, Tzyy-Ping Jung, Chin-Teng Lin, Kaleb McDowell. "Towards Serious Games for Improved BCI ." 9 Sept 2015. Springer Link. <https://link.springer.com/referenceworkentry/10.1007/978-981-4560-52-8_4-1>.
Elisabeth V. C. Friedrich, Neil Suttie, Aparajithan Sivanathan, Theodore Lim, Sandy Louchart, Jaime A. Pineda. "Brain–computer interface game applications for combined neurofeedback and biofeedback treatment for children on the autism spectrum ." 3 July 2014. Frontiers in Neuroengineering. <http://journal.frontiersin.org/article/10.3389/fneng.2014.00021/full>.
Ivan Martinovic, Doug Davies , Mario Frank , Daniele Perito, Tomas Ros , Dawn Song. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. 2012. <https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/martinovic>.
Jaeyeon Jung, Byung-Gon Chun ,Anmol Sheth, William Enck ,Patrick McDaniel, Peter Gilbert ,Landon Cox. Realtime Privacy Monitoring on Smartphones. <http://www.appanalysis.org/>.
José del R. Millán, Frédéric Renkens, Josep Mouriño, Wulfram Gerstner. "Brain-actuated interaction." 26 May 2004. ScienceDirect. <http://www.sciencedirect.com/science/article/pii/S0004370204000967>.
Karlin Bark, Emily Hyman, Frank Tan, Elizabeth Cha, Steven A. Jax, Laurel J. Buxbaum, and Katherine J. Kuchenbecker. "Effects of Vibrotactile Feedback on Human Learning of Arm Motions ." 2 June 2014. US National Library of Medicine National Institutes of Health. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4623827/>.
Kirsten Wahlstrom, N. Ben Fairweather, and Helen Ashman. "Privacy and Brain-Computer Interfaces." March 2016. ACM Digital Library. <http://dl.acm.org.ezproxy.library.uvic.ca/>.
Laurent George, Anatole Lecuyer. "An overview of research on “passive” brain-computer interfaces for implicit human-computer interaction." 17 Nov 2010. Inria. <http://people.rennes.inria.fr/Anatole.Lecuyer/GEORGE_LECUYER_ICABB2010.pdf>.
Law, The Committee on Science and. Are Your Thoughts Your Own?: “Neuroprivacy” and the Legal Implications of Brain Imaging. 1 June 2005. <http://www.nycbar.org/pdf/report/Neuroprivacy-revisions.pdf>.
Leeb R, Sagha H, Chavarriaga R, Millán Jdel R. "A hybrid brain-computer interface based on the fusion of electroencephalographic and electromyographic activities. ." 24 March 2011. US National Library of Medicine National Institutes of Health. <https://www.ncbi.nlm.nih.gov/pubmed/21436524>.
Moor, James H. "The Ethics of Privacy Protection ." 1991. Illinois Digital Environment for Access to Learning and Scholarship.

<https://www.ideals.illinois.edu/bitstream/handle/2142/7714/librarytrendsv39i1-2h_opt.pdf?sequence=1>.
QianQian Li, Ding Ding, Mauro Conti. "Brain-Computer Interface Applications: Security and Privacy Challenges." 7 Dec 2015. IEEEXplore. <www.ieeexplore.ieee.org>.
Peter Brunner, Anthony L. Ritaccio, Joseph F. Emrich, Horst Bischof, Gerwin Schalk. "Rapid communication with a "P300" matrix speller using electrocorticographic signals (ECoG) ." 7 Feb 2011. Frontiers in Neuroengineering. <http://journal.frontiersin.org/article/10.3389/fnins.2011.00005/full>.
Takabi, Hassan. "Firewall for Brain: Towards a Privacy Preserving Ecosystem for BCI Applications." Oct 2016. IEEEXplore. <www.ieeexplore.ieee.org>.
Tamara Bonaci, Howard Jay Chizeck. "Privacy by Design in Brain-Computer Interfaces." Feb 2013. University of Washington. <https://www2.ee.washington.edu>.
Tamara Bonaci, Ryan Calo, and Howard Jay Chizeck. "App Stores for the Brain - Privacy and Security in Brain-Computer Interfaces." 23 May 2014. IEEEXplore. <www.ieeexplore.ieee.org>.
Thorsten Zander, Christian Kothe, Sabine Jatzev, Matti Gaertner. "Enhancing Human-Computer Interaction With input from Active and Passive Brain-Computer Interfaces." 2010. Springer LInk. <https://link.springer.com/chapter/10.1007%2F978-1-84996-272-8_11#page-1>.

Added Work

All the above.

Removed Work

Cynthia Dwork, Moritz Hardt, Toniann Pitass, Omer Reingold, Richard Zemel. "Fairness Through Awareness." 30 Nov 2011. Cornel University Library. <https://arxiv.org/pdf/1104.3913.pdf>.
Jean-Pierre Hubaux, Ari Juels. "Privacy is dead, long live privacy ." Communications of the ACM June 2016: 39-41.
Kamp, Poul-Henning. "More Encryption Is Not the Solution." 30 July 2013. <http://queue.acm.org.ezproxy.library.uvic.ca/>.
Lars Backstrom, Cynthia Dwork, Jon Kleinberg. "Wherefore Art Thou R3579X? Anonymized Social Networks, Hidden Patterns, and Structural Steganography." 8 May 2007. <http://dl.acm.org.ezproxy.library.uvic.ca/>.
Shmatikov, Vitaly. "Anonymity is not privacy: technical perspective ." Communications of the ACM December 2011: 132-132.
Tyson, Peter. "The Hippocratic Oath Today ." 27 March 2001. <http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html>.

1: http://www.thehealersjournal.com/gamma-waves/