Privacy of biofeedback human interfacing devices

Brendan Philip Beauchamp, Lindsay Corneal, Nabeeh Kandalaft
School of Engineering, Grand Valley State University, Grand Rapids Michigan, United States

Article Info

Article history:

Received Sep 8, 2021
Revised Feb 1, 2022
Accepted Mar 22, 2022

Keywords:

Human interfacing devices
Personally identifiable Information
Personal health information
Line drawing

ABSTRACT

The public and governmental focus have been shifted increasingly onto data and privacy due to Facebook's standoff with Apple and several Nations' Governments. An imperative for the discussion of data handling has been made, while Biofeedback human interfacing device (HID) companies such as CTRL-labs and Neuralink introduce new risks in the access, use, and control of personal health information. This paper combines the lexicon of digital self-extension with line drawing analysis to help visualize the industry use of personally identifiable information (PII). Through this analysis encapsulation methods of users' PII have been identified such that discussion of encrypting personal health information (PHI) can be facilitated through analogy. To reduce the likelihood that companies generating biometric hardware are subject to future legal action through laws analogous to European Privacy Law, it is in their best interest to be transparent with their users about data sharing, and educate them on how the companies encrypt their PHI. Should users consent to the use of biometric hardware, this process validates the user control of their own PHI.

Corresponding Author:

Brendan Philip Beauchamp
School of Engineering, Grand Valley State University
301 West Fulton Street, Grand Rapids, Michigan 49504, United States
Email: beauchab@mail.gvsu.edu

1. INTRODUCTION

The work problem, in recent years there have been several new human interfacing devices introduced to the market. These devices use electrical signals from the nervous system and translate them into a computer digestible format to interface with a human more naturally. These systems introduce new dynamics of biofeedback with devices, as a training technique for a device–not explicitly medical treatment [1]. Considering that these technologies are historically biomedical, there is not much discussion written about their application to industry.

While companies are targeting the nervous system interfacing in different domains, these signals extract information about the user which can describe intent, and control devices [2]. The two most prominent companies working on input vectors in this field are Neuralink and CTRL–labs [3]. These companies are working on a brain-computer interface (BCI) and surface electromyographic (sEMG) human-machine interface (HMI) respectively, and allow for high bandwidth input with computers. The most prominent company working on an output vector in this field is Oculus, the company is designing virtual reality visualization tools which increase the output bandwidth of computers to users. While it is exciting to see new technologies shaping the world such as these, many of them communicate data that is not covered in conventional law.

While there are international discrepancies in data ownership, under American Law, social networking sites (SNS) are not subject to personal health information privacy laws such as the health insurance portability and accountability act of 1996 (HIPAA) [4]. In HIPAA, national standards were made such that covered entities must respect personal information privacy controlled by the consent of the subject of that information. Covered entities are explicitly defined as healthcare providers, health plans, healthcare clearinghouses, or business associates of healthcare providers. Modern American Law for amending HIPAA into the internet of things (IoT) has not reanalyzed which entities should be considered covered entities; thus, many companies make their own ethical decisions about the handling of user private data.

Facebook CEO Mark Zuckerberg was brought in front of the United States Congress to discuss his information privacy and their industry dominance [5]. Facebook currently owns the largest messaging service on the planet with WhatsApp, Instagram, Oculus, and CTRL-labs but is not considered a covered entity under HIPAA. Because Facebook is an American company, the data which is stored on Facebook's servers is not enforced to the same level of privacy as an organization that is a covered entity. Despite this, Facebook has shown good work in protecting the privacy of users. Because new technologies are developing faster than laws to control them, it can be difficult to discuss the medium in which these devices operate. There are no limitations to the inferences that a model can make about an individual, and users are not educated well enough on the data which is collected about them.

The solution to the work problem, in regards to the company, it is important to understand that many SNS provide their services for free in exchange for data transactions with advertisers. Specifically, Facebook, their main services have always remained free. While it is important for companies to have users, who understand the personally identifiable information (PII) which is shared about them [6], it is also important for the sake of competition to keep a company's algorithm private.

An individual using an electromyography (EMG) device as a general neural interface communicates data describing the unique kinematics of their hands [7]. In this, a conflict of interest is realized between user data transparency and algorithm propriety. One issue in this discussion is that there is not a universal model for describing the translation from sEMG to the fingertip workspace. In this paper, the workspace translation defined in "A low-cost sEMG development platform for hand joint angle acquisition" is used to visualize PII derived from sEMG wristband devices.

In the context of collecting fingertip workspace or any high bandwidth interfacing vector, data is unique to users manifested through biological differences. This system designed by Beauchamp *et al.* defines the fingertip workspace as the flux of musculoskeletal force acting on the skeletal structure of the hand [7]. This system is expressed in (1), where (qi) is a vector defining the workspace of the fingertips, $\phi(\mathscr{F})$ is a vector defining the flux of forces on the fingertip workspace, while $\mathfrak{G}$ represents a system of matrices which project the joint angles of the hand into space. The translation from musculoskeletal force to fingertip workspace is visualized in Figure 1.

$$\omega(q_i) \fallingdotseq \phi(\check{\mathcal{F}}) \otimes \mathcal{G} \tag{1}$$

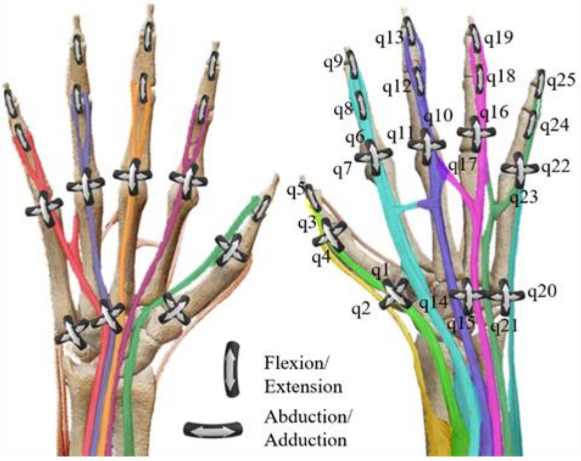

Figure 1. The workspace of the fingertips

Expanding $\mathfrak{G}$ projection matrices from muscle force to joint angle, local, global frame (M, T, and H respectively) shown in (2) and solving for the translation from muscle force to joint angle yields (3). While this is a projection for a normal translation, there are unique scaling coefficients for hand length and handbreadth defined in matrices T and H. Furthermore, there is a unique relationship between an individual's muscle force and the respective output gesture. In this way, the workspace of a user’s fingertips is surface equivalent to the flux of their musculoskeletal force through the unique tensor of their hand.

$$\mathcal{G} \equiv [M\ T\ H] \tag{2}$$

$$M = \frac{\omega(q_i)}{[T\ H]}\left[\phi\left(\check{\mathcal{F}}\right)\right]^{-1} \tag{3}$$

Third-party wisdom about interactions with the digital workspace could manifest themselves in similar ways to modern advertisements, but feel intrinsically different because the company is extracting these inferences through historically biomedical technology. In consideration of the muscle force translation coefficient, algorithms could realize symptoms of carpal tunnel or arthritis and advertise treatments without the user knowing how a company learned this about them. Because this equation is for a normalized translation into the workspace, a personally unique coefficient ***Ꞗ*** is defined which is unique to the individual as shown in (4). While hand length and handbreadth are simple statistics about a user, a muscle force translation coefficient is a more complex structure and says more information about the user. While this is an example, users need to recognize that a company can infer more infer about an individual by combining data and processing it through models which are likely proprietary and hidden from the user. Third-party clarity in the sharing of these unique inferences is imperative in the protection of an individual's PII.

$$\text{Ꞗ}M = \frac{\omega(q_i)}{[T\ H]}\left[\phi\left(\check{\mathcal{F}}\right)\right]^{-1} \tag{4}$$

Literature review: i) Biomedical data and privacy ethics. The dawn of privacy ethics was Aristotle’s polis and Oikos's distinction between politics and the public sphere of politicians respectively [8]. The earliest use of statistics was in the Han dynasty in 2 AD. In 717 AD statistics was used in Arabia for cryptography, and in the 1500s the Western World began developing applied probability and random processes. It has been almost 2500 years since the advent of privacy ethics while using statistics for event analysis is a relatively new technology. Even more modern, the advent of artificial intelligence (AI) and its’ use in human interfacing device (HID) has made the discussion of biomedical data privacy immediately relevant.

Through the development of SNS and online advertising, the commoditization of data has incentivized the collection of detailed digital persona. In parallel to the development of statistical tools for analyzing large collections of data, medical philosophers have defined principles of bioethics that are useful in guiding the discussion of SNS handling biomedical data. In these principles of autonomy, nonmaleficence, beneficence, and justice are defined such that the user is safe from harm, and allows the user to make well-informed, rational decisions about their data [9]. The principle of justice is often quoted by Aristotle as “giving each what they are due” [9], this applies to both the SNS and the user. The user is incentivized to share their data with third-party companies so that they receive the benefits of the HID system. If the company designing the system is deemed to have unethically used user biomedical data in the future, it could result in tremendous litigation. Current HIPAA violations max out owing USD 1.5 million per year and up to 10 years in jail [10].

ii) Secondary use of health data. In the summit meeting toward a national framework for the secondary use of health data, one of the guiding principles agreed upon was the necessity of discussion on privacy policies for secondary use of health data [4]. HIPAA and the health information technology for economic and clinical health (HITECH) Act have made significant strides in moving personal health information (PHI) online and mediating the privacy of this information through the expansion of the Breach Notification Rules and the introduction of violation tiers. These rules provide incentives to covered entities to retain user privacy by increasing multiple case penalties [10], [11]. Despite this though, HITECH did not modify the definition of covered entities, meaning that SNS are not required to follow regulations in these laws unless they receive PHI through a transaction with a covered entity.

Noted once again from the summit, focusing national and state attention on corner cases such as this help protect the privacy of secondary use of health data [6]. While many SNS use the rights and ethics of the individual in the encryption and privacy of user data, it is important to recognize that they are not obliged to legally through HITECH or HIPAA, but are doing so through free will. Addressing differentiations comprehensively like this helps clarify questions related to secondary use of health data [6], and shows that protection of this data through SNS fits the good work's model by going what is legally required of a company handling user data [8], [12].

iii) Digitally extended self and sharing workspace data. In the context of bodily integrity, it is important to consider protocol transparency in the control of secondary health data. Purely in the context of Risk Analysis, protocol transparency generates more detailed information because auditors are capable of generating more advanced event trees. Observing in (4) and Figure 1 the general form of a human hand can be seen in the digital workspace. Using a digital self-extension lexicon, this information becomes part of the digitally extended self when shared online. Figure 2 shows the digitally extended self-model for the interaction between one business and one user [13].

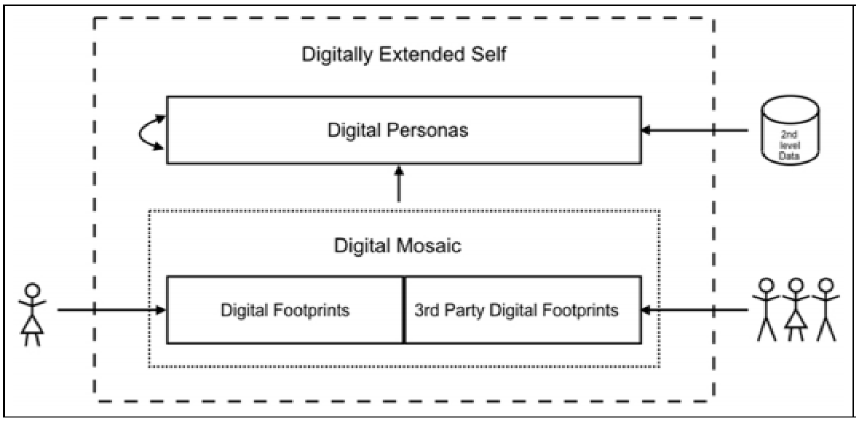

Figure 2. Digitally extended self-model [13]

Considering the 2021 lawsuit over Apple blocking Facebook data popups [10], [14], the contrast between views of data as a commodity and user privacy was presented to the public. It is common knowledge that terms and conditions are commonly skipped through. This is the fault for not educating users about data privacy and shapes the lens through which concurrent generations see their online privacy. It is important to consider the magnitude of data that is collected about users, and the depth of the digital personals generated through internet communication. In internet communication, two types of biomedical data contribute to the digitally extended self: i) those which can be extracted from comparison with a normalized model and ii) those which are inputs to the model.

The benefit of providing a distinction between different types of data and the gradient to their need for encryption is that it provides the opportunity for smaller companies to still have access to data to make their web services more user-centric. While SNS use user data as a commodity with advertising companies, they also use information gathered about the user for improving the platform. This is why Safran *et al.* emphasize the discussion of control of this data, opening the discussion of control emphasizes the user's bodily integrity while understanding that the intricacies of the transaction are multifaceted and need discussion [6].

The most pervasive factor in the model is the consent of the user to process their biomedical data. This though is implied the understanding of the user. IEEE code of ethics cannons I.1 states that engineers are expected to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment [15]. Specifically considering the relationship Facebook has with its advertisers, Facebook makes an effort to protect the privacy of its users through encapsulation of the advertisement process in the platforms model for the digitally extended user. The advertisement criterion is not shared with companies, nor is user data stored.

Furthermore, the code encourages public education on technology's potential consequences to achieve informed consent. Making engineers' first obligation is to the public's safety coincides with Safran *et al.* in their precedence to increase public awareness of secondary use of biomedical data, while most codes of ethics agree that public safety is the highest call of duty overriding all other obligations. Another important note from the code is the importance of informing the public of the qualifications of protecting user data, in the context of algorithm transparency, users would benefit from the increased scrutiny of security. Disclosure of qualifications for encryption would provide checks and balances to the safety structure of encrypting biomedical data.

2. FACEBOOK

Companies like Facebook rely on collecting personal data as a commodity. Due to Facebook’s magnitude of data collection, Mark Zuckerberg was brought to testify before congress for concerns about data monopoly [5]. Facebook has been making news from 2020 to 2021 for battling over data encryption with other tech companies. Facebook has over the past decade become the largest SNS service in the world and is proactively becoming a leader in the next generation of interfacing devices through its ownership of Oculus and CTRL-labs. Despite Facebook's apparent good work in maintaining privacy, their lack of coverage in HIPAA is concerning in consideration of the flexibility of their privacy policy. Facebook’s business model is distributing third-party ads to users for income.

While the topic of privacy is integral to the discussion of personal health information, there are significant discrepancies in the handling of this data in different nations. Due to the moral ambiguity of the topic, experts organized a summit toward a national framework for the secondary use of health data. Members of this summit recognized the growing gap between public and expert knowledge of personal data, and made a recommendation to “focus national and state attention on the secondary use of health data [4]”. Facebook’s acquisition of CTRL-labs is significant in that the company designed an HID using electrical signals from the forearm which are historically health data. While the user owns their neurons, they consent to Facebook using their sEMG data when they wear and use the CTRL-labs wristband.

Facebook is known for its business relationships with online advertisers. The privacy-centric system which has been designed by Facebook and integrated by many other companies is analogous to lobbying in the sense that Facebook connects demographic-based advertisements and individuals without ever disclosing personal health information to advertisers [16]. While this has been understood through terms of service agreements with the platform, CTRL-labs furthers clarity by stating that if a user would like to retain their privacy, they can opt-out of using their device [7].

As HID input increases, its distinction from biometric information has trended to decrease. In the context of Apple’s control of Facebook’s data acquisition, it is important to recognize that user consent is the most important arbiter of use [13]. Facebook’s data policy has made it clear that they do not sell PII to third-party advertisers [16]. From the perspective of Facebook, the company has developed a new technology that increases the benefit to users of HID and increases the rate at which Facebook can harvest data. This is not only a benefit to learning a digital persona about a user for advertisement, but can help distinguish bots from humans by allowing Facebook to track mouse movements [16]. In consent to terms of service, consent to the formation of a digital persona is implied, meaning that using Facebook allows them to make money off of the data which you share with them.

Facebook is a company that makes money from your data [16]. They correlate your digital persona to advertisements that they can display back to you for profit. Facebook vs Congress culminated in the question of whether or not the company was acquiring too much personal data. Congress did not mention anything about the purchase of the company CTRL-labs in the hearing, but it was decided that Facebook was operating under fair practice [5].

3. THIRD-PARTY USE OF PHI AND PII

Modern HID is rapidly evolving. Discussion of these devices is clouded by volatile ethical discussions around privacy and the use of new data types. In order to increase the value of discussion on the topic of modern HID, analytical methods must be quantified for the capacity of analysis. Two models were investigated for discussion; namely, risk analysis and line drawing. While risk analysis would be a superior analytical technique with a more transparent discussion of third-party protocols, line drawing proved more useful in discussion for its effectiveness as a comparative tool between case studies.

3.1. Risk analysis

Risk analysis is an analytical model which quantifies risk through failure modes. These failure modes are ways in which a structure, mechanism, or process can malfunction and manifest themselves through event trees. This model quantifies risk as to the product of the likelihood and the magnitude of harm as well as the inverse of safety [12]. As shown in Figure 3, it is an example event tree with associated probabilities for events.

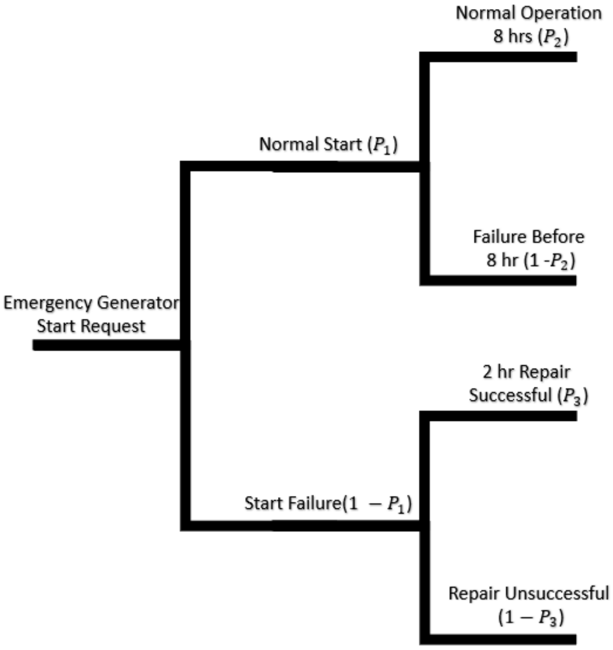

Figure 3. Example of risk quantification

In Figure 4, a model for a communication system is outlined. Disregarding noise introduced in the channel and in the consideration of communicating with a social network service (SNS), a message flows from the user (source) to the SNS (sink) at which point it is processed by the SNS advertisement algorithm. In (1) shows a method of quantifying the information content of a message [16], this information is subsequently used to help the SNS create user-oriented advertisements by targeting topics that have high information content to advertise. The concern is that in this data lies PHI; even if advertising is encapsulated, target SNS can still be hacked for this information content [17].

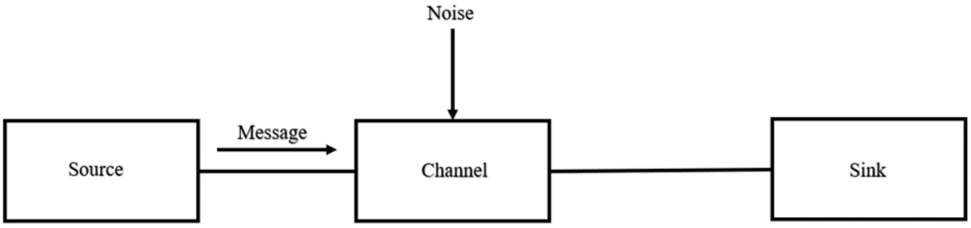

Figure 4. Model of a communication system [16]

$$I(A) = \log_2\left(\frac{1}{P[A]}\right) = \log_2(1) - \log_2(P[A]) = 0 - \log_2(P[A]) = -\log_2(P[A]) \quad (5)$$

In quantifying risk for a system, it is much easier to quantify risk when the architecture of the system is known. Models in which the architecture is known are called a white box, while the black box represents systems in which the inner data flow is unknown. It is important to understand that many web-based companies keep their algorithms black box for competition. This makes it difficult to analyze systems using traditional risk analysis practice. Because it is much easier to foresee potential misuse of a system when the architecture is known, risk analysis is not a sufficient method for discussion.

3.2. Line drawing

Because discussion of privacy is congested in semantics, line drawing serves as a useful tool for comparison to resolved events. In the United States, the collection of PII and PHI is legal for companies who use data as a commodity if they lack coverage in HIPAA. Still, the ethical permissibility of this action is questionable through a conflict of interest in knowledge disclosure. In order to develop a better understanding of the emergent HID technology compares to historical data transactions, three ethical areas of interest have been discussed with respective paradigms. These paradigms are influenced by the recommendations from Safran *et al.*, modern international privacy considerations, the IEEE code of ethics, and digital self-extension. These three ethical subjects will be used in later sections to analyze several companies for their transaction with users. Lastly, the paradigms will be used to analyze CTRL-labs and Neuralink's data policies.

The first ethical topic was educating users on consent to terms of service. It is common knowledge that users consent to terms of service without reading them in order to access services. The positive paradigm is considering the best-case scenario on user education to personal data usage; therefore, it is that the user is kept wise to third party interaction with their digital personal. Inversely, the negative paradigm would be that the user is unaware of the terms of consent. The highest order of magnitude towards the positive paradigm would be keeping active discussion of data usage consistent with the user. In this way, social networking sites cannot amend their privacy policy without notifying the user.

The second ethical subject of the investigation was the privacy of PHI. International differences in privacy legislature are important to recognize in this paradigm because while the European Union has had PHI protection [18], American law does not protect users from PHI collection by social networking sites. In this regard, the positive paradigm would be that PHI is kept completely private by the third party. The negative paradigm would be that PHI is not kept private for the user.

The third area of interest investigated was the subject's benefit to third-party data collection. The positive paradigm in this situation would be that the subject to data collection directly benefits from the data which is collected from them. The negative paradigm would be that the subject dies due to the data collection performed. Observing the effect of third-party data collection on subjects is crucial in this analysis as the health and safety of the individual are of utmost importance in the majority of ethical codes. Table 1 shows PHI use by third-party paradigms.

Table 1. PHI use by third-party paradigms

No	Paradigm		Decision
1.	Educating users on consent to terms of service	+	The user is kept wise to third party interaction with their Digital Persona
		-	The user is unaware of the Terms of Consent
2.	Privacy of PHI	+	PHI is kept completely private within the Third Party
		-	PHI is not kept private for the User
3.	Subject's benefit to third-party data collection	+	The subject of data collection directly benefits from the information which is collected from them
		-	The subject dies due to the data collection performed

3.2.1. Verkada security breach

The Verkada Security Breach involved 149,000 security cameras within the startup becoming accessible to hackers its line drawing analysis is shown in Table 2. Andrew G. Ferguson of American University Washington College of Law emphasized the tradeoff made when security is automated, any security system has its intrinsic security flaws. These cameras were placed inside banks, gyms, and health clinics where users would walk by them. While health information was not explicitly released by Verkada, private health information such as hospital rooms could be recovered [19].

Table 2. Line drawing-Verkada security breach

Paradigm	Decision
1.	Users are not immediately aware of consent when walking by security cameras
2.	Users' health information could be recovered, not explicitly released
3.	Users have increased safety at the cost of increased surveillance

3.2.2. Nazi hypothermia experiments

Between June 1942 and May 1943 Nazi scientists performed experiments on prisoners of Dachau with the intent of investigating the limits of human survival in cold environments. In these experiments' prisoners were forced to participate in several studies involving rapid heating, frigid water, and the elements. The prisoner's responses to these experiments were used to aid in the Nazi war agenda, while in total between 80 to 90 people died. These experiments are historically the worst handling of PHI and are useful as a boundary for line drawing. Table 3 shows the decision paradigm of Line drawing–Nazi Hypothermia experiments.

Table 3. Line drawing–Nazi hypothermia experiments

Paradigm	Decision
1.	Subjects were aware that they had no consent
2.	User health information was shared publicly
3.	Subjects died because of the experiments

3.2.3. Medical devices

Medical devices such as Parkinson's neurostimulators, heart implants, and prosthetics have a direct benefit to the user. The user-device relationship ranges from mutual to commensal, where the user always benefits from the device. The third-party may or may not benefit from data collection. These devices are directly protected by HIPAA, striking a balance between important use of health information and protecting the privacy of those needing healing. Table 4 shows the decision paradigm of line drawing–medical devices.

Table 4. Line drawing–medical devices

Paradigm	Decision
1.	Users are made explicitly aware of consent to service with a health care provider
2.	Users' health information is explicitly kept private by the third party
3.	The user has agreed to use a medical device because it provides aides the user's condition

3.2.4. Siri

Siri is Apple's AI voice companion for their cellphones. It learns information about its user in order to improve the AI – Human relationships. The company has had privacy leaks in the past, though they are a current industry leader in user privacy. Table 5 shows the decision paradigm of line drawing–Siri.

Table 5. Line drawing–Siri

Paradigm	Decision
1.	Users are offered to read terms and conditions but do not have to
2.	Information is currently private
3.	Data shared "improves user experience"

3.2.5. Facebook

Facebook has made it very clear that they use user data as a commodity, despite this; they strive for good work in user privacy. Their advertisement system attempts to completely encapsulate user data, though the company has been subject to hacks over the years releasing troths of user PII. Table 6 shows the decision paradigm of line drawing–Facebook.

Table 6. Line drawing–Facebook

Paradigm	Decision
1.	Users are offered to read terms and conditions but do not have to
2.	Data is kept within Facebook's ecosystem for advertisement
3.	Data is used as a commodity

3.2.6. Privacy as a commodity-Nord VPN (public company)

Nord VPN is a company that sells internet anonymity as a commodity. It is one of the leading web encryption companies on the market and is a byproduct of America's stance on privacy not being a right. Table 7 shows the decision paradigm of line drawing–Nord VPN

Table 7. Line drawing–Nord VPN

Paradigm	Decision
1.	Terms and conditions are easily accessible
2.	The only non-private data is that needed to make the service function
3.	Data shared to improve the user experience or makes task work

3.2.7. Privacy as a commodity–Mobile heartbeat (healthcare communications)

Mobile heartbeat is an encrypted communication company that is targeted at hospitals. The system allows workers at the hospital to have a HIPAA encapsulated communication channel throughout the building. Table 8 shows the decision paradigm of line drawing–mobile heartbeat.

Table 8. Line drawing–mobile heartbeat

Paradigm	Decision
1.	Terms and conditions were actively hidden from the user
2.	PII is shared with other HIPAA compliant companies for advertisement
3.	Data sharing is a source of income for the company, user is advertised treatments

3.2.8. Biofeedback HID–Neuralink

Neuralink is a company started by Elon Musk designing a brain-machine interface (BMI) to be implanted into the skull. While they have had no clinical trials and no safety data on humans, their website has extensive research on the device and allows visitors to learn a lot about the technology. Table 9 shows the decision paradigm of Line drawing–Neuralink.

Table 9. Line drawing–Neuralink

Paradigm	Decision
1.	Information is compact on the website, the theory is discussed, ability to contact
2.	The applications page directly addresses device security
3.	The device will increase human-machine interfacing

3.2.9. Biofeedback HID–CTRL-labs

CTRL-labs has considerable safety data on humans, and significant human trials, and has a developer kit available on their website. The system seems to have gained a lot of momentum and is near public release. Table 10 shows the decision paradigm of Line drawing–CTRL-labs.

Table 10. Line drawing–CTRL-labs

Paradigm	Decision
1.	Privacy is accessible easily, black box user data protocol discussion, ability to contact
2.	User personal information is de-identified, then shared
3.	The device will increase human-machine interfacing

3.3. Discussion of Biofeedback HID and user privacy

The emergence of Biofeedback HID promises revolutionary vectors of device control and is a testament to human engineering. Similar to any new technology, it is important that the associated risk in the device is accurately portrayed to the user. For many users, personal data transactions are understood as a gate to the use of a tool; for others, data sharing is considered insignificant. This means mentalities are dangerous when considering HID processing biological signals because the technology is so unknown. The lens through which personal data discussions are viewed is shaped by a user's history with data privacy. Decisions made about these technological bridges between biomedicine and social networking will set the precedence for future innovations.

Figure 5 shows a graph of line drawing analysis comparing Biofeedback HID (c) to currently available technologies. In regards to the quantity versus depth of analysis of the case studies, it was of utmost importance in designing this line drawing analysis to convey the lens through which modern companies interact with personal information. Through the necessity of conveying this lens accurately, increasing the number of case studies was deemed significant.

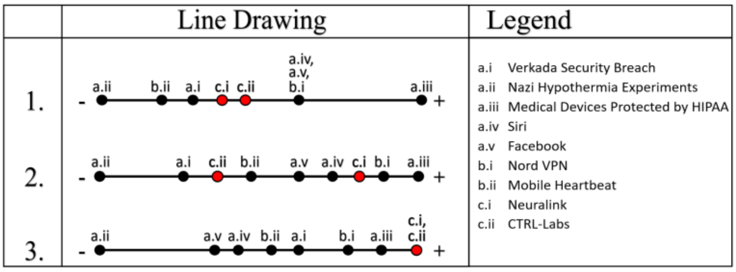

Figure 5. Line drawing analysis for PHI paradigms

4. TERMS AND CONDITIONS OF BIOMETRIC DATA

4.1. Privacy of personal health information

When considering what kind of health information protections people should expect to have, it is important to remember that users consent to data collection before the use of the technology. The issue with expecting data protection in the age of its commoditization is that different nations have laws regarding PHI ownership. Because there is a disparity between international determinations of privacy, there are no clearly defined metrics for providing users with data privacy analysis. In general, people can expect to have significantly less control over a targeted advertisement in companies that are giving their services for free or low price, but the extent of information sharing can only be determined through an analysis of terms and conditions within the company.

The public health emergency privacy act (PHEPA), which was introduced to the senate in 2020, is a step in emphasizing the control of the user. While the act recognizes the benefits of health data collection, it emphasizes the control of the user in ownership of PHI by requiring the deletion of the data after the health crisis is over. The mandate of reports on civil rights infringement is very important in increasing human interfacing bandwidth [20]–[25]. If the public is not accurately informed on a technology, civil rights, and ownership can slip through the cracks of lexicon and protocol black boxing.

From a utilitarian perspective, net good is increased by sharing information with a third party for whom service is desired. While there is a gradient of services and utility of different data types, there needs to be an interdisciplinary discussion on the regulations of PII and PHI use by third parties. In order for the limiting of data to provide benefit to the economy and to encourage new development in the industry, there needs to be an incentive for new companies to collect data. Data handling should take into consideration the quantity of data within the company, furthermore, consideration should be made for what type of data is being handled. There is a significant difference in the information that can be acquired from likes on posts versus conversations between the psychological analysis algorithms of Neuralink and gesture control of CTRL-labs. Ethical committees need to open discussion on PHI usage from entities that are not covered by HIPAA.

One solution is for companies to focus efforts on the encryption of biometric coefficients of users on hardware. In this manner, a user’s unique differences from normalized human data are encrypted on hardware. This follows the process of Safran *et al.* by focusing on ongoing discussions on data access, use, and control [8]. If a user has control over hardware to encrypt their personal information, it could reduce algorithm efficiency, but would support IEEE I.1 in focusing efforts on user privacy. Encrypted middleware would give individuals the assurance that their biomedical data is not being shared with undesired third parties.

4.2. Questions of biometric data ethics

Table 11 contains questions formulated during the research of biomedical data ethics. It is important in the discussion of privacy to consider the evolution of normative behavior. For young people getting exposed to the internet, data transactions are becoming more and more prevalent. This exposure shapes the lens through which they view PII privacy. Going forward from this paper it aspires that these questions help visualize the lens through which the authors viewed PII privacy.

Table 11. Questions of biomedical data ethics

No	Questions
1.	Can private companies give low-cost health care without expecting patients to provide them with valuable data?
2.	At what point in the transformation to the virtual workspace is personally identifiable information encrypted?
3.	How much information is needed to identify a user?
4.	What has history said about privacy?
5.	If discussion shouldn’t focus on data ownership, does that mean that it is owned by whoever owns the storage which possesses the data?
6.	Will collecting personal health information become useful in distinguishing between bots and humans?
7.	Is it ethical for medical privacy as commodity companies to sell user PHI to HIPAA compliant companies for advertisement?

5. CONCLUSION

CTRL-labs and Neuralink are investing resources into unique technology which will change the trajectory of how humans communicate, learn, and perform life. It is important to remember that the decisions made about privacy today shape the lens through which future privacy discussion arises. Facebook has done good work for a non-HIPAA-covered entity, but as human interfacing bandwidth increases, protocol transparency should be enforced in order to improve the public trust and avoid accidental release of PHI. Given that these technologies are very new, vulnerabilities are yet to be exploited. In the current climate of events in data ownership, accidental release of personal information is a daily occurrence. As system architects look forward to the design of future HID, they must look back to the history of privacy and consider the integrity of the individual in the virtual realm.

REFERENCES

[1] D. L. Frank, L. Khorshid, J. F. Kiffer, C. S. Moravec, and M. G. McKee, “Biofeedback in medicine: who, when, why, and how?,” *Mental Health in Family Medicine*, vol. 7, no. 2, pp. 85–91, 2010.

[2] R. Merletti and D. Farina, “Surface Electromyography: Physiology, Engineering and Applications,” *Surface Electromyography: Physiology, Engineering and Applications*, pp. 1–570, 2016, doi: 10.1002/9781119082934.

[3] M. Samuels, “Privacy Policy,” *Commercial Contracts for UK Companies: Formation to Exit*, 2021, doi: 10.5040/9781526511980.precedent9.

[4] R. M. Caplan, “HIPAA. Health Insurance Portability and Accountability Act of 1996.,” *Dental assistant (Chicago, Ill. : 1994)*, vol. 72, no. 2, pp. 6–8, 2003.

[5] HEARING BEFORE THE UNITED STATES SENATE and COMMITTEE ON THE JUDICIARY, “Testimony of Mark Zuckerberg Facebook, Inc.,” 2020.

[6] C. Safran *et al.*, “Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper,” *Journal of the American Medical Informatics Association*, vol. 14, no. 1, pp. 1–9, 2007, doi: 10.1197/jamia.M2273.

[7] B. P. Beauchamp, C. P. Vollmers, M. M. S. Shahriar, and N. Kandalaft, “A Low Cost sEMG Development Platform for Hand Joint Angle Acquisition,” *11th Annual IEEE Information Technology, Electronics and Mobile Communication Conference, IEMCON 2020*, pp. 485–491, 2020, doi: 10.1109/IEMCON51383.2020.9284889.

[8] J. DeCew, “Privacy,” *Stanford Encyclopedia of Philosophy*, 2021.

[9] D. P. Mareiniss and D. Casarett, “Principles of Bioethics,” *Palliative Medicine*, pp. 88–93, 2009, doi: 10.1016/b978-0-323-05674-8.50021-9.

[10] Indiana University, “What are the penalties for violating HIPAA?,” *Knowledge Base*, 2015, [Online]. Available: https://kb.iu.edu/d/ayzf.

[11] “HIPAA and HITECH,” *HIPAA Journal*, 2021.

[12] and M. J. R. C. E. Harris, M. S. Pritchard, M. J. Rabins, R. W. James, “Engineering ethics: concepts and cases, 6th ed,” *CENGAGE*, 2019.

[13] B. Parkinson, D. E. Millard, K. O’Hara, and R. Giordano, “The digitally extended self: A lexicological analysis of personal data,” *Journal of Information Science*, vol. 44, no. 4, pp. 552–565, 2018, doi: 10.1177/0165551517706233.

[14] Josh Taylor, “Facebook v Apple: the looming showdown over data tracking and privacy | Facebook | The Guardian,” *The Guardian*, 2021, [Online]. Available: https://www.theguardian.com/technology/2021/feb/14/facebook-v-apple-the-looming-showdown-over-data-tracking-and-privacy.

[15] “IEEE code of ethics,” *IEEE Transactions on Reliability*, vol. R-33, no. 1, pp. 14–14, 2013, doi: 10.1109/tr.1984.6448267.

[16] M. A. Parsons, “Data policy,” *Data Science Journal*, vol. 12, 2013, doi: 10.2481/dsj.GRDI-008.

[17] H. Simons, “Leaked phone number reveals even Mark Zuckerberg is on Signal,” *Android Authority*, 2021, [Online]. Available: https://www.androidauthority.com/mark-zuckerberg-signal-1215333/.

[18] “Data protection in the EU - Consilium,” *European Commission - European Commission*, 2021, [Online]. Available: https://www.consilium.europa.eu/en/policies/data-protection-reform/.

[19] D. Patterson, “Hack of video security company Verkada exposes footage from 150,000 connected cameras,” *CBS News*, 2021.

[20] R. Blumenthal, “S.3749 - 116th Congress (2019-2020): Public Health Emergency Privacy Act.”

[21] A. Valdez, “A Call to Action for 2021,” *Teaching and Learning in Nursing*, vol. 16, no. 1, pp. 1–2, 2021, doi: 10.1016/j.teln.2020.10.001.

[22] “CTRL-labs – Neural Interface Technology,” *CTRL*, 2021, [Online]. Available: https://www.ctrl-labs.com/.

[23] “Laser-Based Audio Injection on Voice-Controllable Systems,” *Light Commands*, 2021.

[24] “Official Legal Text,” *General Data Protection Regulation (GDPR)*, 2019, [Online]. Available: https://gdpr-info.eu/.

[25] B. P. Beauchamp and N. Kandalaft, “HD-sEMG for Human Interfacing Devices,” *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019*, pp. 519–522, 2019, doi: 10.1109/IEMCON.2019.8936298.

BIOGRAPHIES OF AUTHORS

Brendan Philip Beauchamp is a student at Grand Valley State University pursuing his articulated B.S.E./M.S.E. in Computer Engineering and Biomedical Engineering. He can be contacted at email: beauchab@mail.gvsu.edu.

Dr. Lindsay Corneal iD 8 SC P earned a BASc (applied science) in Mechanical Engineering with a Materials option from the University of Windsor (Canada), an MBA from Lawrence Technological University, and a Ph.D. in Materials Science & Engineering from Michigan State University. She also spent six years as a product engineer at Stellantis Chrysler (now Chrysler, LLC) where her main responsibility was the power steering system for the Ram pick-up truck. She can be contacted at email:corneall@gvsu.edu.

Nabeeh Kandalaft iD 8 SC P received the B.Sc. degree in physics from the University of Jordan, Amman, Jordan, in 1987, and the B.Sc. and M.Sc. degrees in electrical and computer engineering from Iowa State University, Ames, Iowa, in 1991 and 1993, respectively. He received the Ph.D. degree in electrical engineering from the University of Windsor, Windsor, ON, Canada in October, 2012. He was a Post-Doctoral Research Fellow at Teledyne DALSA, Bromont, Canada. He currently is an Assistant Professor at Grand Valley State University, Grand Rapids, MI. His current research interests include Embedded systems, bioengineering, analog/RF integrated circuit design, high frequency testing, microelectromechanical devices, and test methodologies for 3-D integrated circuits. Dr. Kandalaft is a member of the Professional Engineers Ontario. He can be contacted at email: kandalan@gvsu.edu.