Biometrics and Data Privacy: An Analysis of Policies

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

Grace Huang
Spring, 2020

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

Biometrics and Data Privacy: An Analysis of Policies

Biometric Technology and Policies in the United States

What if you never needed to remember a password ever again? With the use of biometrics, or the use of biological measurements that can be used to identify individuals, this reality is not too far away (*What are Biometrics? | Pros and Cons of Biometrics | Kaspersky*, n.d.). Currently, the use of biometrics in personal electronics is quite common. For example, the newest iPhones can be unlocked using Face ID, a feature that uses facial recognition to authenticate users. (*About Face ID advanced technology*, n.d.). In addition, users can log into their laptops using either fingerprint or facial recognition through features such as Windows Hello (*Biometric Facial Recognition – Windows Hello—Microsoft*, n.d.). Since this technology is becoming more universal, it is important to understand and investigate the policies that regulate the collection and use of biometric data. In addition, this type of data may expose sensitive and identifiable information if its collection is not well-regulated. Thus, it is critical that user information is kept private and is not misused.

Currently, there is no federal policy that regulates the collection and use of biometric information in the United States (Stewart, 2019a). Some states have passed their own policies regarding this topic, but the majority have not. States that have implemented their own laws about biometric data privacy do not have a consistent approach; what may be legal in one state may not be in another (Stewart, 2019a). By investigating the social and technological factors that influenced the creation of these laws, the effectiveness of biometric data privacy policies in the United States may be better understood. Alternative policies that better preserve data privacy may also be suggested. By using Thomas Hughes' theory of technological momentum to explain the development of biometric data privacy laws, the following STS research question is

answered: How did social and technological factors influence the creation of biometric data privacy policies in the United States, and why is the inception of these laws significant?

Policy Analysis for Investigating Biometric Data Privacy Laws

This research paper answers the following STS research question: How did social and technological factors influence the creation of biometric data privacy policies in the United States, and why is the inception of these laws significant? To answer this question, this paper conducts policy analysis on current and past regulations regarding the collection and use of biometric data in the United States. The effectiveness of such policies in protecting the privacy of biometric data is also analyzed. To perform this analysis, the paper investigates background information such as when and why such policies were enacted. The information about policies is gathered from state legislature websites. Also, the social context behind these laws is extracted from testimonies from privacy experts and surveys of the general public that were released around the same time that these policies were created. Since this research investigates the relationship between society and biometric technology over time, the sources are organized in chronological order. This paper also reviews specific state laws in question: The Illinois Biometric Privacy Information Act, the Texas Capture or Use of Biometric Identifier Act, and Washington's biometric privacy policy. Policy analysis is the best method to answer this research question because this paper examines laws enacted in the United States. The organization of this data supports an important timeline that demonstrates the relationship between society and technology.

The Significance of Biometric Technology

Biometrics, or a way to measure a person's physical characteristics to verify their identity (Porter, n.d.), is used to log users into a system. This technology provides an alternative means of authentication, or the process that confirms a user's identity. Instead of authenticating users with a piece of information that can be shared, such as a password, biometrics uses a unique physical feature as a means of identification. For example, electronic devices can identify and authenticate users through facial recognition, fingerprint scanning, or even iris scanning (Porter, n.d.). If implemented properly, these new technologies can be faster and easier to use than traditional passwords (Blanco-Gonzalo et al., 2018). Users do not have to remember their passwords for each system they use: all of the information they need to log in is already on their own body.

Currently, biometrics is becoming more widely used. The biometrics market is predicted to reach $30 billion by 2021 (German & Barber, 2017). In addition, it is predicted that 4.8 billion smartphones equipped with biometric technology will be in circulation by 2020 (German & Barber, 2017). Most, but not quite all, consumers are generally accepting of the use of biometrics. In a study from 2018, researchers found that 67% of consumers are comfortable using biometric authentication ("Consumers see biometrics as more secure than passwords, says IBM," 2018). In order for consumers to become more accepting of biometrics, they must be reassured that their data will be kept secure and private. Thus, policies that protect the security and privacy of their biological information must be implemented. Since these methods of user authentication are growing in popularity, it is important to investigate the policies that regulate the collection and use of biometric data. Although biometrics provides an innovative way to authenticate to devices, it also has the potential to expose sensitive biological data if it is not

well-regulated and properly secured. If leaked, this type of information could potentially be used to identify users since it is uniquely linked to each person and cannot be changed easily.

Information privacy has become an increasingly important topic in the past years, even in areas outside of biometrics. Recent events regarding data privacy, such as the Facebook-Cambridge Analytica data scandal, revealed that users' personally identifiable information was being harvested, putting people's online privacy in jeopardy (Fuller, 2018). It was also found that Amazon Echo devices record user conversations. In addition, transcripts of these conversations remain on Amazon servers even if users choose to delete the actual recordings (Barkho, 2019). These events have shown that commonly used pieces of software may not be as secure and private as they should. Privacy protection is especially important with biometric data due to the growing popularity and identifiability of this information.

Currently, in the USA, there is a lack of comprehensive federal policy concerning businesses' collection and use of biometric data privacy (Stewart, 2019a). Although states such as Illinois, Texas, and Washington have laws about the regulation of biometric information, not every state has implemented such policies. Even states that have implemented policies lack consistency in their approach to the issue (Stewart, 2019a). What may be legal in one state may not be in another. Due to this inconsistency of regulations, it is clear that laws concerning biometric data in the United States need to be improved. By investigating how and why these policies came about, the current state of privacy protection of this information is better understood.

Technological Momentum and the Investigation of the Development of Policies

This paper uses Thomas Hughes' theory of technological momentum as a science, technology, and society (STS) framework. This theory is a combination of two other well-known STS frameworks: technological determinism and social construction of technology (SCOT). These two frameworks offer opposing views on the relationship between technology and society. Technological determinism argues that technology influences societal and cultural changes (Hughes, 1994). On the other hand, SCOT argues that the relationship between technology and society is actually reversed. This theory states that society and culture drive and shape the development of technology (Hughes, 1994). Rather than argue one way or the other, Hughes' theory of technological momentum offers an alternative to these two seemingly contradictory theories by considering time as a factor. He states that technological determinism and social construction of technology are true during different stages of maturity of a technology. Society constructs and shapes the development of a technology while said technology is young. As time goes on, the technology becomes more enmeshed in society, gains its own momentum, and begins to drive the development of society (Hughes, 1994). Technological momentum describes the way that technology and society influence each other over time, stating that "social development shapes and is shaped by technology" (Thomas Hughes, 1994).

Critics of this framework argue that this STS theory does not consider the fact that "technology does not acquire such momentum by itself, but rather that interested actors, as institutional entrepreneurs, must launch the technology toward this end" (Wang & Swanson, 2008). These critics also state that success and momentum of a technology when it is first introduced does not guarantee its widespread adoption (Wang & Swanson, 2008). Other critics of technological momentum argue that it is not a unique STS theory, but rather a variant of technological determinism (Vermaas et al., 2011). Nonetheless, technological momentum

provides a good framework to describe the influence technology and society have on each other throughout history.

Since this research paper looks at the development of biometric data privacy policies over time, technological momentum is an appropriate STS framework. The influence that society has on the development of laws regarding biometric technology in the United States is examined, and vice versa. This paper also investigates how this relationship has changed over time.

Through the lens of technological momentum, the interaction between society and technology in the context of biometric data privacy is better understood. The evolution of the relationship between the two entities is also investigated; technology was socially constructed in the beginning stages but evolved over time to become more technologically determined.

The Development of Data Privacy Regulations for Biometrics

Current biometric data privacy policies in the United States are inconsistent due to a lack of federal regulation of the collection and use of biometric information (Stewart, 2019b). Since there is no specific federal policy regulating consumers' biometric information privacy, individual states must implement their own laws to protect their citizens. However, states have varying approaches to these policies. The majority of states have not enacted laws that protect biometric information privacy. Out of the states that have passed biometric privacy laws, some have policies that are more comprehensive than others. The enactment of state biometric data privacy policies demonstrated the relationship between technology and society through technological momentum. The first U.S. policy specific to biometric technology, the Illinois Biometric Information Privacy Act (BIPA), was enacted due to growing concerns about the collection and use of sensitive biological information. This social influence demonstrated the

first phase of technological momentum, where society shaped the development of technology. BIPA would later become the basis of other states' biometric data regulations, illustrating the impact that the Illinois law had on other states' attitudes toward biometric information privacy. This effect demonstrates the latter phase of technological momentum where technology drove the evolution of society. Overall, the social factors that drove the creation of BIPA and the influence of this policy on other states' views towards biometric data privacy show the evolving relationship between technology and society that is described by technological momentum.

Although the United States has enacted some federal regulations for general data privacy, there are none specific to biometric information. These national privacy regulations are typically industry-specific and vary across sectors (Stewart, 2019b). In some cases, these federal policies may be applicable to biometric privacy. However, biometric data is inherently more sensitive and personal than other types of information, since it measures physical features and biological data, and should be treated differently under law (Sherman, 2019). In addition, federal privacy policies are usually not involved in biometric data collection since, in the majority of cases, users who use biometric voluntarily give up their information (Sherman, 2019). As a result, most privacy policies specific to biometric data must be enacted by individual states.

The Illinois Biometric Information Privacy Act became the first state law to address biometric data privacy when it was passed in 2008 (Krishan & Mostafavi, 2018). Under this law, businesses must obtain informed consent before collecting biometric data and may not profit from obtaining biometric information. Businesses must also store data in a secure manner and cannot disclose customers' biometric information unless certain circumstances are met. In addition, companies can only store biometric data until the purpose for collection has been satisfied, or within three years of the customer's last interaction with the business. Lastly, BIPA

creates a private right of action for individuals who may have been affected by a violation of this law (*740 ILCS 14/ Biometric Information Privacy Act.*, 2008). Currently, this is the strictest biometric data privacy policy in the United States (Krishan & Mostafavi, 2018).

BIPA was passed at a time when the general public of the United States expressed discontent with the lack of regulation of biometric information. Many Americans conveyed distrust of this technology due to its novelty and the individuality of this type of data. In a survey conducted in 2004, it was found that 43% of participants considered such technology to be an invasion of privacy (Moody, 2004). Another study revealed that 46% of participants were concerned about new forms of identity theft due to biometric technology. Since biometrics measures physical features such as fingerprints and faces, survey participants were concerned that identity thieves would steal body parts to gain access to private accounts (Elliott et al., 2007). Thus, in order for biometric technology to become widely adopted by the public, users needed to be reassured that regulations were put into place that protected their information.

This public discontent with biometric data privacy is also reflected in BIPA's written statute. Specifically, BIPA states that it was proposed because of the growing use of biometrics in business and the more stringent regulations that such technology requires due to the uniqueness of the data. In addition, BIPA states that the full ramifications of biometric technology are unknown and that the majority of members of the public are wary of the use of biometrics when it is tied to personal information (*740 ILCS 14/ Biometric Information Privacy Act.*, 2008). Since the Illinois law specifically lists public discontent with measures to regulate biometric information as a reason for BIPA's implementation, it is clear that social factors helped to drive the development of biometric privacy laws.

In addition, law experts at the time did not feel that federal policies at the time were sufficient to protect the privacy of consumers' biological information. In fact, experts were urging the United States government to regulate the collection and use of biometric data. In 2008, a few months before BIPA was passed, law professor Peter Swire testified before the United States government, stating that, "Biometrics is the first priority area where I believe that federal privacy policy needs to improve…current protections for biometric information are systematically weak" (*Protecting Personal Information*, 2008). Like the general public, Swire also expressed concern over biological identity theft. He further argued that poor privacy protection of biometric technology could lead to new types of identity theft such as falsified fingerprints (*Protecting Personal Information*, 2008). Other experts at the time stated that the use of this technology was not compatible with federal privacy laws and that states must pass their own legislation in order to properly protect this type of information (Adkins, 2007). These recommendations influenced the development of biometric information privacy, as the first set of laws specific to biometric data was enacted shortly after these pieces of advice were given.

These growing concerns over the privacy of sensitive biological data shaped the development of the first set of biometric regulations in the United States. As outlined in the Illinois Biometric Information Privacy Act, the bill was proposed due to widespread wariness toward biometric technology. At the time that this statute was enacted, there was also growing acknowledgement that privacy laws in the United States were not sufficient to manage the complexity and uniqueness of biological data. Thus, the first privacy policy specific to biometric data in the United States was enacted.

In this way, society shaped the development of this novel technology. This period of time demonstrates the beginning stages of Thomas Hughes's theory of technological momentum.

According to this framework, younger technological systems tend to be influenced by societal factors (Hughes, 1994). This phenomenon is demonstrated by BIPA. This law, which was passed due to influence from the general public and experts in the field, provided guidelines for how businesses were allowed to interact with biometric data. As a result, businesses that developed and used such technology had to adhere to strict regulations. Businesses in Illinois must store biometric data in a secure manner, obtain written consent to collect such information, or risk being sued under this law. During this phase, society drove the evolution of biometric technology.

The years following the enactment of the Illinois Biometric Information Privacy Act illustrated a shift in the relationship between biometric technology and societal influences. This law drove the development of other state-wide biometric privacy policies. In 2009, one year after BIPA was passed, Texas established the Capture or Use of Biometric Identifier Act (CUBI). This policy established many of the same conditions as the Illinois law. Like BIPA, CUBI requires businesses to obtain informed consent before data collection, prohibits companies to profit from consumers' biometric data, store information securely, and destroy the data within a reasonable amount of time (*Texas Business and Commerce Code § 503.001*, 2009). However, one key difference between the two state laws is that while Illinois allows individuals a private right to action, Texas only allows attorney generals to enforce this policy (Sherman, 2019).

Likewise, Washington passed its own statewide biometric privacy law in 2017 (*ENGROSSED SUBSTITUTE HOUSE BILL 1493 as Passed by House of Representatives and the Senate on the Dates Hereon Set Forth.*, 2017). The regulations outlined in this law largely mirror those defined in BIPA and CUBI. Like Illinois and Texas, Washington requires businesses to obtain consent before collecting biometric data and store information in a secure

manner (*ENGROSSED SUBSTITUTE HOUSE BILL 1493 as Passed by House of Representatives and the Senate on the Dates Hereon Set Forth.*, 2017). However, there is one major difference in Washington's privacy policy: entities that collect biometric data for "security purposes" are exempt from the state's guidelines (McCray, 2018).

From the examples above, the effect of technology on society are seen. Based on the similarities in the individual state laws regarding biometrics, the later policies from Texas and Washington were modeled after the Illinois Biometric Information Privacy Act. As described by technological momentum, the relationship between technology and society evolved over time. Prior to the enactment of BIPA, biometrics was relatively novel. Thus, societal influences and attitudes shaped the development of policies concerning this technology. However, as biometrics became more common, more states found it necessary to implement regulations on this technology. As a result, biometric technology began to drive the development of society. BIPA represented a turning point in the relationship between the two, where biometric technology gained momentum and shaped society.

One major limitation of this study is the short time frame in which biometric laws were enacted. Commercial use of biometric technology has only recently become widespread, so the oldest policies concerning the privacy of this type of information in the United States were established less than 12 years ago. In addition, there were few policies to investigate, since most states have not enacted biometric data privacy laws yet. Although the reciprocal relationship between biometric technology and society could be seen through this research, the full effects of technological momentum may further develop over a longer time frame. The time period that is investigated is especially important when using technological momentum, since this STS framework states that the interaction of technology and society evolves over time (Hughes,

1994). Thus, it would be beneficial to continue researching this topic once biometric technology has further matured.

Future studies on biometric data privacy policies may expand on this paper's research by investigating a wider range of laws. Other STS researchers may consider conducting research to compare biometric data privacy laws enacted in other regions, since some countries have more robust privacy policies than the USA. Such an investigation could reveal the interaction between biometric technology and society through the lens of technological momentum on a more global scale. In addition, this comparison of policies could identify favorable privacy strategies in other countries and possibly improve the state of privacy protection in the United States.

The Relationship Between Society and Technology in Biometrics

Current biometric data privacy policies in the United States resulted from a lack of federal guidelines for this type of information, causing individual states to pass their own laws to protect their citizens. Wariness from the general public lead to the establishment of the first biometric data privacy laws in the USA, which would later serve as the basis for policies in other states. The formation of the biometric data privacy policies and the influence of technology and society on each other is seen through the lens of STS. This reciprocal and evolving interaction between biometric technology and society is described by the technological momentum theory. Investigating this relationship is critical to understanding the current state of privacy policies in the United States.

Works Cited

740 ILCS 14/ Biometric Information Privacy Act. (2008). http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

About Face ID advanced technology. (n.d.). Apple Support. Retrieved January 30, 2020, from https://support.apple.com/en-us/HT208108

Adkins, L. D. (2007). *Biometrics: Weighing Convenience and National Security against Your Privacy*. 16.

Barkho, G. (2019, July 5). Amazon Admits Alexa Saves Your Conversations—Even After They're 'Deleted.' *Observer*. https://observer.com/2019/07/amazon-alexa-saves-deleted-conversation-transcripts/

Biometric Facial Recognition – Windows Hello—Microsoft. (n.d.). Retrieved October 16, 2019, from https://www.microsoft.com/en-us/windows/windows-hello

Blanco-Gonzalo, R., Lunerti, C., Sanchez-Reillo, R., & Guest, R. M. (2018). Biometrics: Accessibility challenge or opportunity? *PLoS ONE*, *13*(3), 1–20. https://doi.org/10.1371/journal.pone.0194111

Consumers see biometrics as more secure than passwords, says IBM. (2018). *Biometric Technology Today*, *2018*(2), 2. https://doi.org/10.1016/S0969-4765(18)30016-X

Elliott, S. J., Massie, S. A., & Sutton, M. J. (2007). The Perception of Biometric Technology: A Survey. *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, 259–264. https://doi.org/10.1109/AUTOID.2007.380630

Fuller, M. (2018). Big data and the Facebook scandal: Issues and responses: *Theology*. https://doi.org/10.1177/0040571X18805908

German, R., & Barber, K. S. (2017). *Current Biometric Adoption and Trends*. The University of Texas at Austin Center for Identity. https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf

ENGROSSED SUBSTITUTE HOUSE BILL 1493 as passed by House of Representatives and the Senate on the dates hereon set forth., 6 (2017) (testimony of Cyrus Habib).

Hughes, T. (1994). *Technological Momentum*. The MIT Press.

Krishan, R., & Mostafavi, R. (2018). *Biometric Technology: Security and Privacy Concerns*. 6.

McCray, N. (2018). The Evolution of U.S Biometric Privacy Law. *Insurance Law*. https://www.bradley.com/-/media/files/insights/publications/2018/05/ftd1805mccray.pdf

Moody, J. (2004). Public perceptions of biometric devices: The effect of misinformation on acceptance and use. *Journal of Issues in Informing Science and Information Technology*, 753–761.

Porter, K. (n.d.). *Biometrics and biometric data: What is it and is it secure?* Retrieved October 16, 2019, from https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

Sherman, K. (2019). Biometrics: The Future Is in Your Hands. *Loyola of Los Angeles Law Review*, *50*(4), 663–689.

Stewart, L., lauren. stewart@bc. edu. (2019a). Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security. *Boston College Law Review*, *60*(1), 349–386.

Stewart, L., lauren. stewart@bc. edu. (2019b). Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security. *Boston College Law Review*, *60*(1), 349–386.

Protecting Personal Information: Is the Federal Government Doing Enough?, (2008) (testimony of Peter Swire). https://www.americanprogress.org/issues/courts/news/2008/06/18/4539/protecting-personal-information-is-the-federal-government-doing-enough/

Texas Business and Commerce Code § 503.001. (2009). Findlaw. https://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503-001.html

Vermaas, P., Kroes, P., van de Poel, I., Franssen, M., & Houkes, W. (2011). A Philosophy of Technology: From Technical Artefacts to Sociotechnical Systems. *Synthesis Lectures on Engineers, Technology and Society*, *6*(1), 88. https://doi.org/10.2200/S00321ED1V01Y201012ETS014

Wang, P., & Swanson, E. B. (2008). Customer relationship management as advertised. *Information Technology & People*. https://doi.org/10.1108/09593840810919662

What are Biometrics? | Pros and Cons of Biometrics | Kaspersky. (n.d.). Retrieved January 30, 2020, from https://usa.kaspersky.com/resource-center/definitions/biometrics