2019

The Future of Security: How Biometrics Spell a New Era of Privacy and Security Concerns, and How to Best Protect Citizens Through Comprehensive Legislation

Thomas J. Scrivo

The Future of Security: How Biometrics Spell a New Era of Privacy and Security Concerns, and How to Best Protect Citizens Through Comprehensive Legislation

I. Introduction:

Throughout history, societies have long been plagued with the issue of identification and authentication of their citizens. It was only through proper authentication that the public would know for sure that information was coming from or going to the correct person. For example, in the Byzantine Empire, Lords would only know that an order or decree had come directly from the Emperor Constantine if the letter was signed with the Emperor's unique seal.[1] In addition, identification methods may be used to authenticate that a person attempting to access information limited to a certain audience is indeed who they say they are.[2] For example, many people carry around a driver's license to authenticate that they are the person who appears on the card.[3]

In the present day, we cannot board an airplane without some sort of identification.[4] Additionally, as technology has advanced, our methods of authentication are becoming increasingly digital.[5] Our E-mail, social media, and even online banking cannot be accessed without first setting up and then entering a unique password.[6] However, even as technology has advanced, each of these methods of authentication presents the same serious issue: how can we be sure that the user really is who they say they are? History is flooded with examples of people

[1] http://www.doaks.org/resources/online-exhibits/gods-regents-on-earth-a-thousand-years-of-byzantine-imperial-seals
[2] https://www.miracl.com/press/a-brief-history-of-authentication
[3] Id.
[4] https://www.tsa.gov/travel/security-screening/identification
[5] https://pages.nist.gov/800-63-3/sp800-63-3.html#sec4
[6] https://www.miracl.com/press/a-brief-history-of-authentication

unable to properly authenticate themselves and others impersonating the people they are trying to authenticate. For example, in 1863, members of his own platoon shot General Stonewall Jackson after he was unable to properly identify himself.[7] Additionally, in 1970, Clifford Irving forged letters from tycoon Howard Hughes, and used this to trick McGraw-Hill publishers into purchasing the letters.[8] Even today, many adolescents resort to websites that provide them with fake identification cards to bypass drinking laws.[9]

With an increase in digital and cloud-based information storage, consumers are very vulnerable to hackers who are able to infiltrate and take this information.[10] According to the 2017 Identity Fraud Study, an estimated $16 billion was stolen from 15.4 million U.S. consumers.[11] Even today, things are not improving. On September 11, 2017 consumer credit reporting agency Equifax announced that they had been the victim of the largest cybersecurity data breach in history.[12] Equifax collects and aggregates information for over 800 million consumers and corporations worldwide.[13] Officers at Equifax estimate that cybercriminals accessed personal information from over 145 million users, including names, social security numbers, birthdates, addresses, and even driver's license numbers.[14]

---

[7] Charlton W. Tebeau, *Stonewall Jackson: Confederate General*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/biography/Stonewall-Jackson#toc3626.
[8] *Forgery*, LEGAL DICTIONARY, https://legaldictionary.net/forgery/.
[9] Chris Hayes, *FOX Files Update: Fake ID Website Shut Down*, FOX2NOW (Nov. 20, 2012) http://fox2now.com/2012/11/20/fox-files-website-shut-down-for-fake-ids/.
[10] *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.
[11] Id.
[12] Steve Symanovich, *Equifax Data Breach Affects Millions of Consumers. Here's What to Do,* LIFELOCK (Oct. 12, 2017) https://www.lifelock.com/education/equifax-data-breach-2017/.
[13] Id.
[14] Id.

Additionally, Equifax stated that credit card information and credentials from over 209,000 consumers had been compromised.[15] The 145 million users who had information stolen amounts to almost ten times the number of people who had information stolen throughout the entire previous year. Consumers, government officials, and experts in the field have been looking to other means cybersecurity to help prevent this from occurring in the future because of the sheer amount of information compromised.

One proposed means of enhanced security is the use of biometrics.[16] Biometrics in this sense refers to biometric identifiers, which are any biological characteristic that can be used to identify a person.[17] This most commonly comes in the form of using fingerprints, but it can also encompass retina/iris scanning, facial geometry, and voice recognition.[18] While these identifiers were initially used in criminal investigations, technology has grown to the point where biometric identifiers are used almost every day in commercial settings. For example, iPhones allow users to unlock their phones after inputting their fingerprints.[19] In fact, the recently announced iPhone X allows users to open their phones by scanning the user's face.[20] This announcement is significant because average consumers are more vulnerable as more and more companies use consumers' biometric data.

---

[15] Id.
[16] April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns*, WIRED (March 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.
[17] *Biometric Identifiers*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/biometrics/#bg.
[18] Id.
[19] Thomas Fox-Brewster, *Does Apple Face ID Make It Easier For Feds To Hack The iPhone X? Yes And No*, FORBES (Sept. 12, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/12/iphone-x-faceid-security-danger/#480521f5512d.
[20] Id.

The biometric identifier field is largely unregulated, which gives companies the freedom to store and use an individual's biometric information in any way they please. This has both civil liberty and cybersecurity implications as well.[21] The Electronic Privacy Information Center has identified six major areas of concern when dealing with the collection of biometric information: storage, vulnerability, confidence, authenticity, linking, and ubiquity.[22] To combat this, some states have passed comprehensive legislation that regulates the collection and storage of biometric information.[23] Currently three states (Illinois, Texas, and Washington) have enacted laws that deal with the issues described above.[24]

This note sets out to explore these issues through legislation, research, and case law in order to formulate a model piece of legislation for New Jersey. In Part I, I will discuss the history and uses of biometric information, and the development of the industry that resulted in the issues we face today. In Part II, I will explore the three states that have enacted comprehensive biometric identifier legislation, discussing the advantages and disadvantages of each. In Part III, I will look at the development of recent case law where there have been disputes over the above legislation. Finally, in Part IV, I will use the information discovered above to create a piece of legislation for New Jersey that best protects the privacy and civil liberties of the citizens of New Jersey.

II. Background Overview of Biometrics

[21] *Biometric Identifiers*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/biometrics/#bg.
[22] Id.
[23] Michelle J. Anderson & Jim Halpert, *Washington becomes the third state with a biometric privacy law: five key differences* (June 21, 2017), https://www.dlapiper.com/en/us/insights/publications/2017/06/washington-third-state-with-biometric-privacy-law/.
[24] Id.

The purpose of authentication is to ensure that a user is authorized to access the information or perform the action that he or she is attempting to get or perform.[25] Ideally, this practice is meant to reduce the potential for fraud and misrepresentation.[26] While it is generally easy to authenticate someone in person, the process of electronic authentication presents the challenge of authenticating over a digital network.[27] In order to do this, systems will use one or more authentication factors, which fall into one of three categories: (1) knowledge factors, (2) ownership factors, and (3) inherence factors.[28]

First, knowledge factors would include something like a password or security question.[29] These are factors that the user has knowledge of, and usually will set up with the system when originally creating an account or profile. Next, ownership factors include something that the user actually has in their possession.[30] Examples of ownership factors include ATM cards, identification cards, driver's licenses, one-time password tokens, or even cell phones.[31] Finally, inherence factors include something that a user actually is or does.[32] This is the category that biometric identifiers fall under, and include facial, fingerprint, retinal pattern, and voice recognition.[33]

[25] Id.
[26] Id.
[27] Id.
[28] Id.
[29] Id.
[30] Id.
[31] Id.
[32] Id.
[33] Id.

Different systems use these factors in a variety of ways to increase security.[34] For example, single-factor authentication is a security measure that includes only one component of one of the above factors.[35] This is the least secure method of authentication, as one single factor does not sufficiently defend against intrusion.[36] Another process is called two-factor authentication, which uses a combination of two independent components from two different factor categories.[37] For example, when a user tries to log in to a banking website to perform a financial transaction, he or she would be required to enter a username and password (knowledge factor), as well something from another category.[38] For banking, the second factor is often an ownership factor coming in the form of a one time password sent to a cell phone via text message, or an actual ATM card.[39]

Even more secure than this is multi-factor authentication, which combines two or more authentication factors.[40] A subset of multi-factor authentication is so-called strong authentication, which is similar to multi-factor authentication be necessarily requires the use of digital certificates or other non-replicable factors. The European Central Bank (ECB) defines strong customer authentication as a procedure based on at least two of the three authentication factors (knowledge factors, ownership factors, and inherence factors), and that the individual factors must be mutually independent.[41] Furthermore, at least one of the factors must be "non-reusable

---

[34] *The Differences Between Single and Multi-Factor Authentication*, APPLIED BIOMETRICS INSTITUTE, http://abibiometrics.org/the-differences-between-single-and-multi-factor-authentication.html.
[35] Id.
[36] Id.
[37] Id.
[38] Id.
[39] Id.
[40] Turner, *supra* note 25.
[41] Id.

and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet."[42] By stating factors should be mutually independent, the ECB means that the hacking of one does not compromise the other factors.[43] In addition, "non-replicable" factors means that the factor is only available for a certain amount of time, and once it is used it is no longer valid.[44]

Many groups in United States have used these methods to develop strategies to best authenticate users with success, accuracy, and security. For example, the American National Institute of Standards and Technology outlined a baseline digital authentication model that is best suited for these electronic authentication processes.[45] In this model, an individual (known as an applicant) applies to a credential service provider (CSP) in order to enroll.[46] The enrollment is complete once the CSP has proven the applicant's identity, at which point the applicant becomes a subscriber to the CSP and some sort of authenticator, such as a username, is created.[47]

The role of the CSP is to maintain and protect subscriber credentials, while the role of the subscriber is to maintain their authenticators.[48] As a subscriber, a user can perform any action or transaction once authenticated for a period of time.[49] There will often be transactions within the main session that will require a user to re-authenticate their credentials in order to proceed, adding another wrinkle of protection.[50] Using online banking as an example, the CSP is usually a separate entity from the bank itself.[51] The CSP must verify that a subscriber is authenticated and

---

[42] Id.
[43] Id.
[44] Id.
[45] Paul A. Grassi, *Digital Identity Guidelines*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (June 2017) https://pages.nist.gov/800-63-3/sp800-63-3.html#sec4.
[46] Id.
[47] Id.
[48] Id.
[49] Id.
[50] Id.
[51] Id.

then rely that information to the relying party (in this case the bank) to let them know that the user is authorized to perform a certain transaction.[52] Examining this, it is clear that a CSP has an extremely important role in cybersecurity and authentication.[53] Mistakes on behalf of the CSP, either caused by oversight or hacking, can have detrimental effects on consumers. In an effort to better protect consumers, companies have begun to take steps to increase the security and accuracy of authentication, which comes in the form of biometrics.

Throughout history, societies have used biological characteristics of its inhabitants as a means to identify those citizens. These types of identifiers are extremely important because they are very difficult to replicate and/or forge. For example, there is evidence of Babylonian business transactions in 500 BC being completed via fingerprinting to help authenticate the purchaser and seller.[54] However, modern fingerprinting became mainstream in the late 1800s when Edward Henry, a police investigator in Bengal, India, developed a system (known as the Henry System) to classify people based on their fingerprints.[55]

While fingerprinting and other means of personal identification were used mostly in the physical realm, the roots of merging this concept with technology began to emerge in the 1960s.[56] For a long time, only the government used biometric identifiers. In 1992, the National Security Agency (NSA) created the Biometric Consortium in order "to initiate and/or expand efforts in testing, standards development, interoperability, and government cooperation."[57] Issues

---

[52] Id.
[53] Id.
[54] Lauren Katims Nadeau, *Tracing the History of Biometrics*, Government Technology (Oct. 23, 2012), http://www.govtech.com/Tracing-the-History-of-Biometrics.html.
[55] Id.
[56] *Biometrics History, Nat'l Sci. & Tech. Council*, DEPARTMENT OF HOMELAND SECURITY (last updated Aug. 7, 2006).http://www.biometrics.gov/documents/biohistory.pdf
[57] Id.

with biometric identity and security came to a head following the attacks of September 11, 2001.[58] The United States government realized that biometric identifiers could be crucial in protecting national security.[59] In fact, at the time, Larry Ellison, CEO of Oracle, advocated for a program where each US citizen was given an identification card that included their fingerprint information, as to authenticate the identity of the cardholder.[60]

As technology has grown, the use of biometric identifiers has grown as well. Currently, biometric identification is used in government, military, criminal justice, and private industry to authenticate an individual's identity.[61] Many businesses use biometric information for security and verification purposes. For example, Facebook and Shutterfly use facial recognition to help users tag themselves and friends in photographs.[62] Further, financial services will often use voice recognition or fingerprints in order to verify financial transactions.[63] In addition, telephone companies such as Apple and Android use fingerprinting as a way for a user to unlock his or her phone.[64] The use of biometrics in the consumer sphere will not only not slow down, but will likely increase exponentially as companies continue to integrate identifiers into their products and services.

---

[58] *Biometric Identifiers*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/biometrics/#bg.
[59] Id.
[60] Id.
[61] Id.
[62] *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103 (N.D. Ill. Dec. 29, 2015); *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cali. May 5, 2016).
[63] Penny Crosman, *U.S. Bank Pushes Voice Biometrics to Replace Clunky Passwords*, AM. BANKER (Feb. 13, 2014), http://www.americanbanker.com/ issues/179_31/us-bank-pushes-voice-biometrics-to-replace-clunky-passwords-1065608-1.html [https://perma.cc/MH3Y-4CMC].
[64] Thomas Fox-Brewster, *Does Apple Face ID Make It Easier For Feds To Hack The iPhone X? Yes And No*, FORBES (Sept. 12, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/12/iphone-x-faceid-security-danger/#480521f5512d.

These services are not being entirely forced on consumers, however, as research shows that nearly 70% of consumers would be open to using their fingerprints to make payments while shopping.[65] The thought of using biological identifiers no longer seems "scary" to the general public, who have begun to laud the process for its ease and convenience.[66] As a response, many companies have increased efforts to integrate biometrics into their products and services. For example, in an October 31 press release, American Express announced a new generation of digital authentication that supports biometric identifiers such as fingerprints and facial recognition.[67]

Additionally, banking services are working on offering fingerprint embedded payment cards, which are expected to reach 160 million shipments by the year 2022.[68] In fact, even car companies are beginning to use biometrics, and it is estimated that one in three cars will feature some sort of biometric integration by the year 2025.[69] These features can include a fingerprint scan to start the car, sensors to sense when a driver is impaired, and blood pressure and body scans to minimize distractions while driving.[70] With increasing demand for biometric integration, it seems like an optimal situation for consumers. Users are acquiring increased ease of access to

---

[65] Clare McDonald, *Almost 70% of customers willing to use fingerprint biometrics to shop,* COMPUTERWEEKLY (Oct. 24, 2017) http://www.computerweekly.com/news/450428775/Almost-70-of-customers-willing-to-use-fingerprint-biometrics-to-shop

[66] Id.

[67] Andrew Johnson, *American Express Supports Next Generation of Digital Commerce Over Internet-Connected Devices With SafeKey® 2.0 Rollout,* AMERICAN EXPRESS (Oct. 31, 2017) http://about.americanexpress.com/news/pr/2017/amex-next-generation-digital-commerce-with-safekey-rollout.aspx.

[68] ABI Research, *Biometric Payment Cards to Boost Banking Industry Security,* PR NEWSWIRE (Nov. 7, 2017) https://www.prnewswire.com/news-releases/biometric-payment-cards-to-boost-banking-industry-security-300550424.html.

[69] Kayla Matthews, *Biometric Vehicle Access is Only a Matter of Time,* FINDBIOMETRICS (Nov. 2, 2017) https://findbiometrics.com/biometric-vehicle-access-411029/.

[70] Id.

different transactions and information, all while better protecting that information...or so they think.

Several large problems will reveal themselves as the use of biometrics continues to grow. One major issue is the security of stored biometric information. Stored biometric information has a higher value to those seeking to steal someone's identity because biometric information is very difficult to change.[71] For example, information like passwords, phone numbers, and credit card numbers can easily be changed, so they do not have as much value.[72] However, information like medical records, social security numbers, and biometric identifiers cannot be changed, and therefore yield a much higher price on the black market.[73] Security remains a paramount issue because over the past year, the Federal Trade Commission (FTC) reported almost 400,000 complaints of identity theft.[74] A percentage of these complaints were over stolen biometric information, such as fingerprints, retina scans, and voice recognition.[75] From this biometric information, hackers can recreate a fingerprint or voice in order to gain access to very private information, and it is very difficult to differentiate a hacker from the verified user.

It is simple to recognize why many people might think that biometric information will be extremely difficult to hack and use. People often think how it is difficult to imagine how someone can remotely take something that is unique to your biological person and use it to impersonate you. However, that is exactly what is happening. For example, in 2014, hackers

---

[71] Id.
[72] Id.
[73] Karen Gullo, *What are the risks of biometric identification?,* ELECTRONIC FRONTIER FOUNDATION (Feb. 28, 2017) https://www.eff.org/mention/what-are-risks-biometric-identification.
[74] https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints
[75] Id.

working for the Chinese government hacked computer systems that stored personnel information, including the fingerprint data of 5.6 million people.[76] For people still skeptical how this information could be converted to a means to actually access information, hackers have taken care of that as well. In fact, researchers at Michigan State University created fake fingerprint scans using special paper and a standard inkjet printer, which were used to fool smartphone fingerprint readers.[77]

Even more alarming, a person need not even have inputted his or her fingerprint information into a database for it to be compromised. Researchers at Tokyo's National Institute of Informatics reconstructed fingerprint models using a photo of an individual flashing a peace sign.[78] Methods do not even have to be this complex, as some hackers have even used Play-Doh to create fingerprint molds to fool almost 90 percent of fingerprint readers.[79] These methods are not only limited to fooling fingerprint scanners. Because many facial recognition systems are at their infancy in terms of accuracy, there have been instances where a hacker bypassed facial recognition software of a Lenovo laptop by simply holding up a photograph of the user.[80] This same technique has been found to be effective with iris-scanning systems as well.[81]

Furthermore, hackers are exploiting weaknesses in security systems that many companies use when storing voice biometrics.[82] When a customer phones in to a call center and is told that

---

[76] Kaveh Waddell, *When Fingerprints Are as Easy to Steal as Passwords*, THE ATLANTIC (March 24, 2017) https://www.theatlantic.com/technology/archive/2017/03/new-biometrics/520695/.

[77] Id.
[78] Id.
[79] Marc Goodman, *You Can't Replace Your Fingerprints*, SLATE http://www.slate.com/articles/technology/future_tense/2015/02/future_crimes_excerpt_how_hackers_can_steal_fingerprints_and_more.html.
[80] Id.
[81] Id.
[82] Id.

his or her call may be recorded for quality assurance, they are agreeing to have their biometric data used.[83] From these voice recordings, companies will create a biometric roadmap, similar to what facial scans do with a photograph, to measure satisfaction based on the pitch, volume, and tone used by the caller.[84] Again, these advancements represent the mere tip of the iceberg in terms of advancements in biometric technology. In fact, Motorola has partnered with MC10, a firm specializing in wearable medical technology, in an effort to "extend human capabilities through virtually invisible wearable electronic RFID tattoos" which will be used for authentication.[85] Additionally, the company Proteus Digital Health has been developing a pill that, when swallowed, interacts with stomach acid to create a unique signal and uses the entire body as a password.[86] Even knowing this, it will be difficult to remain ahead of hackers who desire to obtain a person's biometric information. Thus, it is important to look toward experts in the field for guidance in how to tackle the issues that come with increased use of biometric data.

The United States government and related agencies have needed to adapt to the increased prevalence and pervasiveness of hackers. One way that organizations in both the public and private sectors are accomplishing this is by actually hiring hackers to infiltrate their network.[87] For example, companies such as Google, Pintrest, and Western Union have used hackers to test the abilities of their network security.[88] Further, each year there are hacking conferences held around the world which brief both commercial and government leaders about the prevalent issues in hacking and how to best prepare them. One of the most prominent of these conferences

---

[83] Id.
[84] Id.
[85] Id.
[86] Id.
[87] *Hack my network- please*, CBS NEWS (Feb. 23, 2015) https://www.cbsnews.com/news/companies-hire-hackers-to-break-into-their-systems/.
[88] Id.

is known as Black Hat.[89] Black Hat was founded in 1997 by hacker Jeff Moss, who also founded popular hacking competition DEF CON.[90] At Black Hat 2015, Dr. Thomas P. Keenan presented an explanation of the risks associated with biometric identifiers and how to best avoid them.[91]

Besides the obvious risks associated with any sort of information procurement, Keenan highlighted seven "hidden risks" associated with increased use of biometrics.[92] First, he highlighted biometric reliability and the public perception of it. He explained how many consumers either think that technology works or does not work, so if they see biometrics being hacked they will lose trust.[93] However, the flip side is that if they are assured that biometrics are secure, they will not remain vigilant against hackers.[94] The second hidden risk is a lack of discussion of the consequences of errors involved in biometric technology. Because of the nature of biometrics, many people do not realize that these systems are plagued with the same issues as any other digital authentication systems (Type I Errors known as false rejections, and Type II Errors known as false acceptances).[95]

Another risk of biometric identification is the implications of the irreversible nature of biometric data. This risk echoes the concerns that many have already expressed in that it is impossible to change biometric data once it is given. The fourth risk that is discussed is the issue of consent. There are many companies that specialize in obtaining facial models from people just

[89] http://www.blackhat.com/html/bh-about/about.html
[90] Id.
[91] Dr. Thomas P. Keenan, *Hidden Risk of Biometric Identifiers and How to Avoid Them*, CANADIAN GLOBAL AFFAIRS INSTITUTE, https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf.
[92] Id.
[93] Id.
[94] Id.
[95] Id.

by observing them in a public place.[96] Further, as discussed later in the paper, there are many different laws across different jurisdictions in the U.S. that make it difficult to enforce regulations on companies looking to obtain biometric information without user consent.[97] An additional risk associated with biometrics is that biometrics are not only associated with something that we "are", but also things that we "do." It is this behavioral aspect of biometric screening that can be inaccurate and cause issues with false positives and false negatives.[98] The sixth risk that is given is that as biometrics increase in prevalence, it may soon become de facto necessary to be enrolled in some sort of biometric identifier. For example, India has begun developing the world's largest biometric database for its 1.3 billion citizens, and enrollment is required if a citizen wants the benefit of any government-run services in India.[99] Therefore, while technically optional, it is likely that no citizen would refuse government services to protect their biometric rights.

In fact, at Disney World Resorts, they sell MyMagic wristbands, which track your movements and behaviors.[100] While guests can opt for the standard park admission ticket, guests will miss out on many of the perks that MyMagic wristband holders are entitled to, thus making it de facto mandatory to obtain these wristbands. Additionally, many insurance companies such as Allstate have released driver-tracking apps that are offered in exchange for driver insurance discounts.[101] Finally, other insurance companies are offering incentives to provide them with biometric information. Insurer John Hancock currently offers discounts on insurance to

---

[96] Id.
[97] Id.
[98] Id.
[99] http://www.latimes.com/world/la-fg-india-database-2017-story.html
[100] https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf
[101] Id.

customers who wear fitness monitors, which provide information about a person's exercise and sleeping habits.[102] Finally, and most importantly, biometrics includes the risk of data thieves and aggregators. Like any other type of digital information, biometric information is susceptible to theft and alteration. One risk that many are unaware of is that there are many companies that act as aggregators who cross over their biometric information with other companies. For example, 23andMe, a consumer DNA testing site, shares much of its biometric information with Genetech, a large pharmaceutical company.[103]

Because of many of these concerns, the Federal Trade Commission (FTC) has established some guidelines and suggestions for companies who obtain and store biometric information.[104] The FTC is an independent agency operated by the United States Government that focuses mainly on consumer protection.[105] In this case, the FTC wrote a repot about what companies who obtain facial scans should do with that information.[106] The main goal of that report was to help companies establish practices and policies to help protect consumer privacy.[107] The FTC recommended three major points in its report. First, they urged companies to design their services with consumer privacy in mind.[108] Next, they recommended that companies develop adequate security precautions to protect the information they collect, including where to store the information and how to dispose of the information when it is no longer needed.[109] Finally, they

---

[102] Id.
[103] Id.
[104] *FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies*, FEDERAL TRADE COMMISSION (Oct. 23, 2012) https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition.
[105] *About the FTC*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/about-ftc.
[106] https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf
[107] Id.
[108] Id.
[109] Id.

warned companies that facial data is extremely sensitive, and to be wary about where and how these systems are set up (recommended that technologies should not be set up in places where children congregate).[110]

Further, the FTC preached the importance of consumer consent. They state that a company should make sure that its customers are aware when they are opting in to facial recognition programs, and give them the option to refuse.[111] Such notice is crucial in enabling average consumers to best protect their own private information, as it gives them the option of whether or not they want their facial scans stored with said company. Specifically, the FTC warned that social media companies should provide consumers with clear warnings that the consumers are opting into facial recognition services.[112] Further, the social media company should provide a means for consumers to opt in and out of these services as they please, and to have any biometric data that had been stored on servers permanently deleted.[113]

This policy, as we will discuss later, demonstrates incredible foresight by the FTC, as this very recommendation could have saved companies such as Facebook time and money in future litigation. Of course, the FTC is an independent government agency, and can only provide recommendations to and state and federal governments. As of 2017, there is no comprehensive federal law scheme dictating what companies can and cannot do with consumer biometric information. However, there are three states that have ratified legislation dealing with these exact issues, and they will be discussed in turn.

III. Current State Laws

[110] Id.
[111] Id.
[112] Id.
[113] Id.

A. Illinois Biometric Information Privacy Act (BIPA)

In the early 2000 a company called Pay By Touch began the long awaited trek for companies looking to expand into biometric authentication.[114] It promised to link various user accounts, including credit cards and checking accounts, under one system that could be accessed by a user fingerprint.[115] While this technology seemed promising and garnered the support of hundreds of millions of dollars worth of investment funds, the project ultimately fizzled out due to poor operations and management.[116] What this fallout did provide, however, was a glimpse into the future of authentication. Using this, the Illinois government realized that the use of biometrics in the commercial world was fast approaching, and they needed to act quickly in order to ensure that their citizens were well protected. Thus, in 2008, the Illinois legislature introduced the Illinois Biometric Privacy Act ("BIPA").[117]

In fact, during hearings on the enactment of the bill in the Illinois House, Representative Joseph M. Lyons stated,

> [t]his legislation is needed because we've seen examples of biometric use in stores. Pay By Touch is the commonly used vendor at Jewel grocery stores and their affiliates. This company marketed themselves as being secure and having a safe place to keep the biometric information it collects. However, it filed for bankruptcy in 2007 and wholly stopped providing verification services in March 2008, leaving the customers who had signed on for this program in Albertsons, Cub Foods, Farm Fresh, Jewel Osco, Shell and

[114] Justin O.Kay, *The Illinois Biometric Privacy Act,* ASSOCIATION OF CORPORATE COUNSEL http://www.acc.com/chapters/chic/upload/Drinker-Biddle-2017-1-BIPA-Article.pdf.
[115] Id.
[116] Id.
[117] 740 Ill. Comp. Stat. Ann. 14/5.

Sunflower Market without any information as to how their biometric and financial data will be used.[118]

Enacted in October of 2008, BIPA was revolutionary at the time.[119] The law recognizes the crucial right of an individual to his or her privacy of biometric information, and as such allows for redress when companies misuse, or collect without notice, such information.[120] Specifically, BIPA regulates the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[121] A "biometric identifier" is defined to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," while things like photographs, physical description, written signatures, writing samples, demographic data, and certain biological materials used for medical purposes are excluded.[122]

From this description, BIPA sets out four main points. First, BIPA requires any private entity that desires to collect, purchase, capture, or otherwise obtain a person's biometric identifiers or information to inform that person in writing that they are doing so.[123] Further, this writing must include the purpose for the collection of the biometric information as well as the length of time such biometric information will be collected, stored, and used, and the company must receive a written release from the consumer.[124] Next, BIPA sets limits on what companies can do once they receive biometric information from a consumer. It states that any commercial entity in possession of biometric identifiers must refrain from: (i) selling, leasing, trading, or otherwise profiting from such identifier or information; and (ii) from otherwise disclosing or

[118] O'Kay, *supra* note 115.
[119] Id.
[120] 740 Ill. Comp. Stat. Ann. 14/5
[121] Id. at14/5(g)
[122] Id. at 14/10
[123] Id. at 14/5(b)
[124] Id.

disseminating such information unless the person consents, the disclosure completes a financial transaction authorized by the person, or the disclosures is required by law or requested via warrant or subpoena.[125]

Furthermore, BIPA establishes rules for how and to what extent private entities must safeguard the biometric information that they collect. Any company in possession of biometric information must "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry."[126] This standard of care must be at least "the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."[127] Finally, BIPA requires companies to adhere to its rules regarding retention and eventual destruction of biometric information. It states that each private entity must develop "a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."[128]

One of the most significant features of BIPA is that it creates a private right of action for any citizen aggrieved by a violation of any of the above provisions.[129] This can be a right of action in a state circuit court or as a supplemental claim in federal court against the offending party. Any party who prevails against an offender may recover liquidated damages or actual

[125] Id. at 14/5(c)-(d)
[126] Id. at 14/5(e)
[127] Id.
[128] Id. at 14/5(a)
[129] Id. at 14/20

damages, whichever is greater.[130] This right of action has become one of the most important aspects of BIPA, as it has spurred litigation against a variety of private commercial entities including Google, Facebook, and Shutterfly.

From 2008 on, BIPA served as model legislation for the protection of consumer biometric information. In 2009, Texas passed a similar law called the Capture or Use Biometric Identifier Act, which used many of the same principles as BIPA, but did not include a private right of action. Instead, only the Texas Attorney General could bring a claim against a violative party.[131] For years, these were the only two states that passed legislation regarding biometric information, despite several states having active debates. However, that changed in May of 2017 when the state of Washington passed House Bill 1493 (HB1493).

B. Washington Law- House Bill 1493 (HB 1493)

Going into effect on July 23, 2017, HB 1493 became the third law enacted in the U.S. that featured a comprehensive set of regulations for commercial collection of biometric information.[132] HB 1493 does, however, contain several important differences from its predecessors in Illinois and Texas. First, HB1493 focuses on the concept of enrollment of biometric identifiers.[133] Instead of broadly requiring express consent for any collection, use, or disclosure of biometric information, HB 1493 allows companies to "enroll" any biometric identifiers into a database for commercial purposes.[134] This means that biometric identifiers can be collected without consent, but can not be "convert[ed] into a reference template that cannot be

[130] Id.
[131] Tex. Bus. & Comm. Code 503.
[132] Engrossed Substitute House Bill 1493, http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/Session%20Laws/House/1493-S.SL.pdf#page=1.
[133] Id.
[134] Id.

reconstructed into the original output image, and store[d] in a database that matches the biometric identifier to a specific individual."[135] Thus, in order to legally enroll a biometric identifier into a private database for a commercial purpose, a person must (i) provide notice; (ii) obtain consent; or (iii) provide a mechanism to prevent subsequent use of the biometric identifier for commercial purpose.[136]

The second major difference from BIPA is that HB 1493 alters the legal definition of a "biometric identifier," which specifically excludes physical and digital photographs and audio and video recordings.[137] HB 1493 defines "biometric identifier" to be "data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[138]

Additionally, the law specifically makes no mention of facial geometry in its definition of biometric identifiers. This is likely in response to recent lawsuits that have been filed under BIPA that allege companies such as Facebook, Google, and Shutterfly have taken facial geometry information from the photographs that users upload. For example, in the case against Facebook, Plaintiffs filed a putative class action suit stemming from Facebook's "Tag Suggestions" program.[139] When users upload photographs of themselves and others, they usually "tag" other people by clicking on the photo and assigning a name to each individual in the photo.[140] However, Facebook's Tag Suggestions program uses a program to identify a person in

[135] Id.
[136] Id.
[137] Id.
[138] Id.
[139] *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp 3d 1155, 1158 (N.D. Cal. 2017).
[140] Id.

an uploaded photograph based on other photographs of that person that have already been uploaded to the website.[141] This "state-of-the-art facial recognition technology" extracts biometric information from uploaded photos and creates digital representations (known as templates) of people's faces using a geometric map of their facial features.[142] The users, however, were never warned of this practice, and thus did not offer affirmative consent, nor were they even offered the option of refusing the service. Against a motion to dismiss by Facebook, the plaintiffs survived because the court interpreted BIPA to state that these sort of templates fell under the definition of "biometric identifier."[143] It is likely that the Washington legislature explicitly refused to put in the same definition of "biometric identifier" as BIPA to avoid a similar ruling.

Another difference between HB 1493 and BIPA is that HB 1493 has a more relaxed view on the notice and consent requirements.[144] In fact, there is no specific kind of notice or consent that is required prior to enrolling a biometric identifier. The law only states that the exact type of notice and consent required for enrollment is "context dependent," and that "notice is a disclosure, that is not considered affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals."[145] Conversely, BIPA requires affirmative written notice to be provided, and consent may only be granted with the submission of a written release prior to collecting biometric information.[146] While less stringent than BIPA, HB 1493's standard on consent and notice is actually on par with the Obama

---

[141] Id.
[142] Id.
[143] Id. at 1171.
[144] http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/Session%20Laws/House/1493-S.SL.pdf#page=1
[145] Id.
[146] BIPA

Administration and its report on consumer data privacy, as well as the FTC's report on Protecting Consumer Privacy.[147]

Additionally, HB 1493 includes several exceptions to the notice and consent requirements that do not appear in BIPA. HB 1493 is unique in that it exempts the use of biometric information for the purposes of security of fraud prevention.[148] In other words, if the biometric information is used for a "security purpose," there is no notice required to collect, capture, or enroll that biometric data.[149] The law defines a "security purpose" as a means of "preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person."[150] Further, HB 1493 does not require consent prior to selling or enrolling biometric information is a variety of situations. These scenarios include if the sale or disclosure is: (i) consistent with the requirements of the biometric law; (ii) necessary to provide a product or service subscribed to, requested by or expressly authorized by the individual; (iii) necessary to effect, administer, enforce or complete a financial transaction requested, initiated or authorized by the individual and where the recipient maintains confidentiality of the biometric identifier and does not further disclose it; (iv) required or expressly authorized by a federal or state statute or court order; (v) made to a third party who contractually promises that the biometric identifier will not be further

[147] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
[148] http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/Session%20Laws/House/1493-S.SL.pdf#page=1
[149] Id.
[150] Id.

disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the law; or (vi) made to prepare for litigation or to respond to or participate in judicial process.[151]

Finally, unlike BIPA, HB 1493 does not contain a private right of action. Similar to the Texas law, only the Washington Attorney General may enforce the law's requirements.[152] Again, this portion of the law was likely added in response to the large amount of litigation coming into Illinois courts under BIPA. However, it is unclear what groups had influence in forcing this part into the law. It might have been the result of lobbying from corporations, or perhaps it was an effort to keep the docket of Washington judges clean. However, it seems the former is more likely. Some of the largest corporations in the world are headquartered in the state of Washington, including Amazon, Costco, Microsoft, and Starbucks.[153] It is likely that many of these companies, especially the ones heavily involved in social media and digital ventures, would like to limit as much as possible the amount of legal exposure they have as they likely venture into more biometrically integrated projects.

HB 1493 does, however, share important similarities with BIPA. Namely, they both contain similar security and retention requirements. As such, HB 1493 states that a person who knowingly possesses a biometric identifier of an individual: (i) must take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the person; and (ii) may retain the biometric identifier no longer than is reasonably necessary to comply with a court order, statute, or public records retention schedule specified under law.[154] Because it is the most recent legislation that has

---

[151] Id.
[152] Id.
[153] Caitlin Dempsey, *Fortune 500 List by State for 2015*, GEO LOUNGE (July 28, 2015) https://www.geolounge.com/fortune-500-list-by-state-for-2015/.
[154] Id.

passed, HB 1493 provides an interesting look at what current New Jersey legislation might look like.

IV. New Jersey Plan

In 2002, Assemblywoman Joan M. Quigley and Assemblyman Neil M. Cohen introduced legislation to the New Jersey assembly entitled the "Biometric Identifier Privacy Act."[155] Six years before the enactment of BIPA in Illinois, the New Jersey assembly debated on but ultimately did not pass a bill that was supposed to help protect the biometric information of its citizens.[156] The bill included provisions such as: (i) notwithstanding any other provision of law to the contrary, no person shall obtain a biometric identifier of an individual, for the purpose of commercial advantage, without authorization of the individual; and (ii) a person who possesses a biometric identifier of an individual shall not sell, lease, or otherwise disclose the biometric identifier.[157] Similar to BIPA, the law does include several exceptions to the latter rule including if given consent by the owner, if the sale is permitted by law, and to comply with law enforcement.[158] Unlike BIPA, however, the bill states that any person that violates any of the above provisions shall not be liable for a penalty of more than $25,000.[159] In addition to BIPA, this bill also includes similar regulations on what governmental entities can do when they possess biometric information.[160] These damages, unlike those for a private entity, are not limited to $25,000, and a person aggrieved may seek full damages.[161] Additionally, the bill

[155] ftp://www.njleg.state.nj.us/20042005/A1500/1194_I1.PDF
[156] Id.
[157] Id.
[158] Id.
[159] Id.
[160] Id.
[161] Id.

contains a private right of action.[162] Like BIPA and HB 1493, the NJ bill contains language stating that an entity that possesses a biometric identifier shall protect disclosure of that identifier with reasonable care and in a manner that is the same as or more protective than the manner in which the entity stores and protects other confidential information.[163]

To model new legislation in New Jersey, it is important to not only look at other legislation, but to also be reasonable by looking at how to best go about getting something like this passed. Realistically speaking, it will be very difficult to pass legislation that mirrors New Jersey's 2002 bill, as it grants citizens, albeit wholly deserved, hefty recourse for company actions. While many of the existing litigation under BIPA has to do with companies violating the notice and consent requirements of BIPA.[164] While this is important, the more pressing issue is that of security. As we have discussed, there are many risks associated with the use of biometrics, one of them being that once breached they cannot be changed.[165] As such, any New Jersey legislation should have more stringent security requirements than the "reasonable care" standard. Either that, or the "reasonable care" standard should reflect the type of care that certain agencies or organizations deem sufficient. For example, we can look toward reports of the FTC.[166] Also, we can look towards leaders in the cybersecurity field for recommendations.[167]

---

[162] Id.
[163] Id.
[164] *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp 3d 1155.
[165] Karen Gullo, *What are the risks of biometric identification?,* ELECTRONIC FRONTIER FOUNDATION (Feb. 28, 2017) https://www.eff.org/mention/what-are-risks-biometric-identification.
[166] https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf
[167] Dr. Thomas P. Keenan, *Hidden Risk of Biometric Identifiers and How to Avoid Them,* CANADIAN GLOBAL AFFAIRS INSTITUTE, https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf.

Overall, while it might take bargaining with leaders in business, New Jersey could implement more stringent security regulations in exchange for more relaxed consent and notice requirements, similar to the enrollment process of HB 1493. Finally, New Jersey legislation should contain a private right of action, similar to BIPA, with part liquidated damages, or actual damages if the total damages are higher.

V. Conclusion

It is difficult to predict how technology will change, but it is important that our society change with it. Currently, New Jersey has a unique opportunity to get on the forefront of legislation that only three of the fifty states currently have in place. Using these laws as a guide, as well as taking information that continues to be discovered regarding the storage and security of biometric information, New Jersey should be able to craft comprehensive legislation that will protect the information of its citizens, while not completely abandoning its businesses. The future is now, and it is time that New Jersey enters it.