FACING THE FACTS ON BIOMETRIC PHONE LOCKS: YOUR FACE AND THUMB ARE NOT SECURE

Bilal Adra[*]

TABLE OF CONTENTS

I. INTRODUCTION

The technology of BACK TO THE FUTURE has arrived. No, I'm not referring to hover-boards, the Mr. Fusion Reactor, or a fully functioning flying car

[*] J.D. Candidate, University of Illinois Class of 2019. I would like to thank my family and friends for helping to foster my interest in technology, especially as it relates to Computer Science. I would also like to thank Professor Faye Jones at the University of Illinois, for fostering my interest in Data Privacy and Security through her Privacy and Security class at the University of Illinois.

interstate system, although I wish that were the case.[1] I'm referring to the widespread use of Biometric Authentication, the kind used by Jennifer to access her future-self's home.[2] Although these authentication methods are not widely used to access our homes, they are used in an arguably more intimate setting: our smartphones and other personal devices.[3] These days you would be hard-pressed to find a smartphone that doesn't contain some sort of Biometric Authentication mechanism, usually in the form of a fingerprint scanner.[4] Additionally, not including these mechanisms in new phone models is a notion some would find ridiculous.[5] A Biometric Authentication method makes it easier than ever to access your device quickly when compared to PIN's and Patterns, all you need is to touch the sensor and you're in.[6] And, with the iPhone X's new feature, Face ID, all it takes is a glance at your phone to unlock it.[7]

Of course, Biometric Authentication methods, in the form of fingerprint scanners, have been included in smartphones for more than ten years.[8] Their usage has only increased, with just about every flagship phone containing some sort of fingerprint scanner or a similar technology.[9] As a result, we have seen the rise of many different standards and laws concerning the storage and use of this information.[10] However, no laws, regulations, or even industry standards

[1] BACK TO THE FUTURE PART II (Columbia Pictures 1989). In the movie, Marty and "Doc" are busy preventing Marty's future child from committing a crime, while Jenny is left sleeping in a nearby alley. Two police officers find her and take her to her future home, where she gains access to her home using her thumbprint.

[2] *Id.*

[3] Fionna Agomuch, *Password-free Smartphone are No Longer the Stuff of Science Fiction—They're Everywhere*, BUS. INSIDER (Dec. 27, 2017), https://www.businessinsider.com/smartphone-biometrics-are-no-longer-the-stuff-of-science-fiction-2017-12.

[4] *See* Andrew Martonik, *This is Why Sony Phones in the U.S. Don't Have Fingerprint Sensors*, ANDROID CENTRAL (Aug. 31, 2017), https://www.androidcentral.com/sony-fingerprint-sensors-us-deals (finding it "ridiculous" and "bizarre" that Sony has chosen to sell their new phone models in the United States without any fingerprint sensor).

[5] *Id.*

[6] *See Unlock with Your Fingerprint*, GOOGLE [hereinafter *Unlock with Your Fingerprint*], https://support.google.com/pixelphone/answer/ 6285273?hl=en (last visited Oct. 21, 2018) (explaining how to set up and use the fingerprint sensor for the Google Pixel); *see also Use TouchID on iPhone and iPad*, APPLE [hereinafter *Use TouchID*], https://support.apple.com/en-us/HT201371 (last visited Oct. 21, 2018) (explaining how to set up and use Apple's TouchID on the iPhone and iPad).

[7] Glenn Fleishman, *Face ID on the iPhone X: Apple Releases Face ID White Paper and Support Document*, MACWORLD (Sept. 7, 2017), https://www.macworld.com/article/3225406/iphone-ipad/face-id-iphone-x-faq.html (describing Apple's new feature on its iPhone X allowing users to gain access to their phone using their face).

[8] Jayaditya Chakrabarty, *Fingerprint Scanner On Phones: History & Evolution, But Do We Really Need That?*, IGADGETSWORLD (Apr. 17, 2016), https://www.igadgetsworld.com/fingerprint-scanner-history-evolution-but-do-we-really-need-that (describing the history of fingerprint scanners on smartphones and questioning whether it is really a necessary feature).

[9] Samuel Gibbs, *2015: The Year the Fingerprint Sensor Stopped Being a Gimmick*, THE GUARDIAN (Dec. 27, 2015), https://www.theguardian.com/technology/2015/dec/27/2015-fingerprint-sensor-smartphone-security-biometrics-data (describing the widespread adoption of fingerprint sensors in smartphones.

[10] *See generally* Illinois Biometric Information Privacy Act, 740 ILL. COMP. STAT. §14 (2008) (providing guidelines for Illinois Business concerning the use and storage of Biometric Information); *see also* FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012) [hereinafter FACING FACTS], https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies (providing guidelines for the use of facial recognition data); *see also* Ted Claypool & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, AM. BAR ASS'N (May 2016), https://www.americanbar.org/content/dam/aba/publications/blt/2016/05/biometric-info-201605.pdf (providing a brief overview of Biometric Information laws, standards, and regulations).

have been developed regarding how this information should be used to give consumers access to their devices.[11] Further, there have been many instances where researchers were able to trick fingerprint scanners to gain access to user devices.[12] Additionally, financial services are increasingly allowing users to log-in to their accounts and make purchases using Biometric Authentication.[13]

Part II of this Note explores the history of Biometric Authentication, and the current laws surrounding Biometric Information. It explores the flaws and workarounds found for Biometric Authentication in smartphones. The current laws regarding the use of Biometric Information are also described. It also explains how standards in the Technology Industry help create a more secure environment for consumers.

Part III explores the industry's attempts to create a standard regarding the use of Biometric Information for unlocking smartphones and personal devices. It also covers how the current laws are used to protect consumer data, and their flaws when applied to the use of Biometric Information as a passcode. It then explains how the use of a standard would create more secure interface for users.

Finally, Part IV proposes several solutions which could be adopted to create a standard. These range from federal regulations to calling on the industry itself to develop a comprehensive standard when unlocking users' devices with Biometric Identifiers like your face or thumbprint.

II. BACKGROUND

A. Biometric Information Defined and a Brief History

Biometric Information generally refers to information that can identify a person using some sort of physiological or behavioral characteristic.[14] These characteristics are judged by the following requirements: universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention.[15] Some of the more common and useful Biometric Identifiers are: DNA, fingerprints, irises or retinas, the face, ears, and gait.[16]

[11] Natasha Singer, *Consumer Groups Back out of Federal Talks on Face Recognition*, N.Y. TIMES (June 16, 2015), https://bits.blogs.nytimes.com/2015/06/16/consumer-groups-back-out-of-federal-talks-on-face-recognition/?_r=0 (describing the breakdown of talks in a conference to create standards for the use and storage of Biometric Information).

[12] *See generally* Vindu Goel, *That Fingerprint Sensor on Your Phone is Not as Safe as You Think*, N.Y. TIMES (Apr. 12, 2017), https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html (describing several security concerns present in the use of fingerprint sensors as an authentication method).

[13] *See* Nicholas Yeap, *Your Finger is About to Replace Your Bank Password*, CNN: TECH (June 9, 2015), http://money.cnn.com/2015/06/05/technology/bank-fingerprint-reader/index.html (describing how financial institutions are increasingly adopting Biometric Authentication methods).

[14] Anil Jain et al., *An Introduction to Biometric Recognition*, 14 IEEE TRANSACTIONS ON CIRCUITS AND SYS. FOR VIDEO TECH., SPECIAL ISSUE ON IMAGE- AND VIDEO-BASED BIOMETRICS 4 (Jan. 2004).

[15] *Id.* at 14.

[16] *See id.* at 7–10 (comparing several common and useful Biometric Identifiers).

Biometric Identifiers, in the form of fingerprints, have been in use for over one hundred years.[17] The discovery of patterns on fingerprints was first documented by Marcello Malpighi in 1686.[18] However, it was not known that fingerprints were unique to each person until Dr. Henry Faulds published an article which discussed the use of fingerprints to identify individuals in 1880.[19] In 1888, Sir Francis Galton found that fingerprints do not change over the course of one's life, and there is a one in sixty-four billion chance of two individuals having the same fingerprints.[20] Sir Galton also discovered the characteristics which can be used to identify fingerprints, aptly named Galton's Details, which are still in use today.[21] In 1902 the United States began using fingerprints as an identification system, and they have increasingly been used as a means of identification to this day.[22]

The development of digital signal processing in the 1960's allowed the development of computer systems to identify an individual by their fingerprint.[23] In the 1970's the use of hand geometry to provide identification was developed.[24] This was followed by retinal, signature, and facial identification in the 1980's, and iris scans in the 1990's.[25]

B. How Biometric Information is Used in Smartphones

With those breakthroughs in technology, and with the rapid pace of computer development, it is no surprise that these identification systems are small and fast enough to be used in smartphones and other personal devices today.[26] As early as 2007 one of the first smartphones with a fingerprint sensor, the Toshiba G500, was released.[27] However, fingerprint sensors were not prevalent in many phones until Apple's iPhone 5S included one with its release in 2013, and the use of these sensors as authentication for financial transactions began in 2014.[28] With the release of Apple's iPhone X, facial recognition has now become another identification method in our smartphones.[29] Windows

[17] *See* Fingerprint History, U.S. MARSHAL'S SERVICE, https://www.usmarshals.gov/usmsforkids/fingerprint_history.htm (last visited Oct. 20, 2018) (providing a brief history of the use and development of Biometric Identifiers).

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *See id.* (showing that the use of fingerprints to identify individuals in the United States began in the New York Prison system and spread to the military and other parts of the government).

[23] ANIL JAIN ET AL., BIOMETRIC SYSTEMS 2 (Anil Jain et al. eds., 2005).

[24] *Id.*

[25] *Id.*

[26] It is a commonly held notion among Computer Specialists that the power of computers, in processing, memory, etc., roughly doubles every two years because the number of transistors that can fit on a single piece of silicon doubles in that timespan. This notion was first conceived by Gordon Moore, the co-founder of Intel, and is commonly referred to as "Moore's Law," even though it is more of an observation than a law. *See generally* Don Clark, *Intel Rechisels the Tablet on Moore's Law*, WALL ST. J.: DIGITS (June 16, 2015), https://blogs.wsj.com/digits/2015/07/16/intel-rechisels-the-tablet-on-moores-law (explaining what is commonly cited as "Moore's Law").

[27] Chakrabarty, *supra* note 8.

[28] *Id.*

[29] Fleishman, *supra* note 7.

Hello, which was included in Microsoft's Windows 10 operating systems for desktops and laptops, has added the ability to use Biometric Authentication in the form of facial recognition or fingerprint sensors.[30] Microsoft claims this system is three times faster than inputting a password.[31]

With the inclusion of these sensors comes a difference in goals between the end user and the designers of the sensors.[32] Generally, the designers want to create the most secure and accurate method possible for authentication, while the end user wants a fast and easy-to-use system.[33] This difference in goals means that not all Biometric Identification methods can be used, and provides a good reason for the use of fingerprints or facial recognition over more exact methods of identification like DNA analysis which would take more time and processing power to achieve.[34] Device makers are obviously aware of this difference in goals, and to an extent would rather lean towards more ease of use and quick identification to appeal to consumers.[35]

As evidenced by the widespread adoption by manufacturers and users alike, the use of these Biometric Authentication methods provide many benefits to consumers.[36] These benefits include, but are not limited to: user appeal, cost efficiency, and the traits being unforgettable.[37] Additionally, even though most smartphone users are aware of a security PIN or password feature, fewer than fifty percent actually use that feature because of a lack of confidence in such a feature or mere inconvenience.[38] Many smartphone users are more than happy to use an alternative method, like Biometric Authentication, which can be quicker, and in their eyes more secure.[39] Who wouldn't want to be able to swipe their finger or glance at their phone, or other devices, to gain immediate access?[40] After all, it's much easier to forget your password or PIN than your face or fingerprint.[41]

C. The Law Surrounding Biometric Information

As Biometric Information has become more prevalent, governments have realized that there must be regulation concerning the storage and use of this information.[42] It is nearly impossible, at least without extensive plastic surgery, to replace your Biometric Information, unlike passwords or PINs which can be

[30] *See Windows Hello: Discover Facial Recognition on Windows 10*, MICROSOFT, https://www.microsoft.com/en-us/windows/windows-hello (last visited Oct. 20, 2018) (describing a new feature in Windows 10 which allows users to log in with various Biometric Identifiers).

[31] *Id.*

[32] Jain et al., *supra* note 14, at 4.

[33] *Id.*

[34] *Id.*

[35] Yeap, *supra* note 13.

[36] Adrina Pocovnicu, *Biometric Security for Smartphones*, 13 INFORMATICA ECONOMICA 57, 59–60 (2009).

[37] *Id.*

[38] *Id.* at 57.

[39] *Id.*

[40] *Id.* at 60.

[41] *Id.* at 59.

[42] *See* Claypool & Stoll, *supra* note 10 (providing a brief overview of Biometric Information laws, standards, and regulations).

changed at whim.[43] This creates a need for governmental regulation in the space in order to ensure that the Biometric Information volunteered by consumers is not abused.[44]

For students, California and Delaware both have laws restricting the use of Biometric Information and prohibit websites from selling that information.[45] North Carolina and West Virginia prohibit students' Biometric Information from being stored in student data systems.[46] Likewise, Illinois, Arizona, Wisconsin, Louisiana, and Kansas all have laws which prohibit schools from collecting Biometric Information from students without parental consent.[47] Florida, with one of the more comprehensive laws, prohibits schools from collecting, obtaining, or retaining Biometric Information from students, their parents, or their siblings.[48]

Illinois was the first state to implement regulations for Biometric Information collected by businesses through its Biometric Information Privacy Act (BIPA).[49] The Illinois BIPA prevents businesses from selling their customers' Biometric Information, requires informed consent to collect Biometric Information, and gives consumers the right to sue businesses over the misuse of their Biometric Information.[50] Texas and Washington are currently the only other states to pass similar acts.[51]

The Federal Government has not yet passed any similar bill, and no agency has yet to create any similar regulations.[52] However, the FTC has released a document detailing suggestions and "best practices" for the industry to follow, though this only applied to facial recognition data.[53] These best practices are based on three principles: privacy by design, consumer choice in providing the data, and transparency.[54]

The FTC also analyzes several case studies and provides suggestions for how to handle those situations.[55] The first such case study analyzes an eyeglass company which allows consumers to upload pictures of their face in order to try various styles of glasses.[56] The images are stored by the company for the

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Claypool & Stoll, *supra* note 10.

[49] *Id.*

[50] *Id. See generally* Illinois Biometric Information Privacy Act, 740 ILL. COMP. STAT. §14 (2008) (providing a framework of rules and guidelines for businesses to follow when collecting Biometric Information from Consumers).

[51] Claypool & Stoll, *supra* note 10; *see also* H.B. 1493, 2017 Reg. Sess. (Wash. 2017) (a recently passed bill in Washington similar to the Illinois BIPA). *See generally* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2015) (providing guidelines similar to the Illinois BIPA).

[52] Claypool & Stoll, *supra* note 10.

[53] *See* FACING FACTS, *supra* note 10 (providing a variety of practices which could help provide more security in the storage and use of biometric information).

[54] *Id.* at 2.

[55] *Id.* at 11–20.

[56] *Id.* at 11.

consumer to easily use the information again to try different styles at a later date without re-uploading the image.[57]

The FTC recommends that the company take three steps to address the storage and collection of this data.[58] First, it should implement "privacy by design" by securely storing the images and documenting a process to dispose of them after they are no longer needed.[59] Second, the company should "inform consumers of: (1) the length of time the images are stored, (2) who will have access to the stored images, and (3) consumers' rights regarding deletion of the stored images."[60] Finally, if the company should decide to use the images in another manner, like advertising, it should inform consumers of the change and obtain their affirmative consent to use their images.[61]

Another case study covers the use of facial recognition in social networks, where the social network scans photos uploaded by a user and identifies which friends may also be in the photo so they may be "tagged."[62] Here, the FTC gave three recommendations for social networks to follow.[63] First, the social network should ensure that the data and biometric information in the images is stored securely.[64] Facebook's policy of encrypting these images and information is cited as an example of a good policy here.[65] The FTC also states that even if the images are not meant to be used or processed in any way by the social network these precautions should still be taken to prevent unauthorized secondary use of the data.[66]

Second, the FTC states that social networks should have data retention and disposal policies in place, and that these policies should be communicated to the consumer.[67] This should be done through a clear notice to consumers describing these practices, and should give them the option to opt out if they choose to.[68] The social network should also put practices in place to prevent the storage and use of biometric data of non-users, as they have no practical way to opt-out of the use of their images on the network.[69]

Finally, the FTC explains two scenarios where a social network should obtain affirmative consent from users before collecting or using biometric data from images.[70] The first scenario is that the social network, like all other companies, should obtain the consumer's affirmative consent to use that data in any materially different way than it represented when collecting the data.[71] Second, the social network should not identify users who are not "friends" of the

[57] *Id.*
[58] *Id.* at 11–12.
[59] FACING FACTS, *supra* note 10, at 11–12.
[60] *Id.* at 12.
[61] *Id.*
[62] *Id.* at 17.
[63] *Id.* at 17–19.
[64] *Id.* at 17.
[65] FACING FACTS, *supra* note 10, at 17.
[66] *Id.* at 17–18.
[67] *Id.* at 18.
[68] *Id.* at 18–19.
[69] *Id.*
[70] *Id.* at 19.
[71] FACING FACTS, *supra* note 10, at 19.

user when they are uploading the image, even if they are recognized in the photo.[72] This prevents the revelation of someone's identity to someone who is not already known to them.[73]

These case studies do give some guidelines to the industry for the storage and use of biometric information; however, none of the case studies offer advice on how to use that information for authentication, or any best practices for the use of such information in that manner.[74]

D. The Use of Standards in the Technology Industry

In most areas of the technology industry, standards, rather than laws or regulations, play a critical role in the development and commercialization of new technologies.[75] Standards allow for the uniformity and interoperability of technologies, and also allow for more global solutions as they are often internationally adopted among many companies.[76] Examples of some common standards are: USB, WiFi, SMS, and MP3; each of these has allowed varying devices from different manufacturers to connect together and share information.[77]

Standards are developed by various Standard Setting Organizations (SSOs), which are composed of various industry analysts.[78] The analysts are experts in their industries and have a narrowly focused knowledge set which allows them to create and promulgate standards to benefit the industries, governments, and consumers alike.[79]

Additionally, some standards are created and adopted by the Federal Government through NIST (National Institute of Standards and Technology) which is part of the Department of Commerce.[80] NIST works to foster standards in varying technological fields ranging from health records to computer chips.[81] These standards are meant to anticipate the future and promote the development of new technology in the United States.[82]

[72] *Id.*

[73] *Id.*

[74] *See id.* at 11–20 (explaining that the case studies focus on some common uses of facial recognition but are not meant to represent an exhaustive discussion of all uses).

[75] Brad Biddle et al., *The Expanding Role and Importance of Standards in the Information and Communications Technology Industry*, 52 JURIMETRICS 177, 178 (2012); *see also* Stephen Brown, et al., *Electric Vehicles: The Role and Importance of Standards in an Emerging Market*, 38 ENERGY POL'Y 3797, 3798 (2006) (discussing the role of standards in achieving a successful emerging industry, with a focus on the electric vehicle industry); Christopher S. Gibson, *Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in Intellectual Standards*, 22 BERKELEY TECH. L.J. 1403, 1404 (2007) (discussing the interplay of standards and intellectual property and advocating for a system which takes intellectual property and international trade concerns into account).

[76] Biddle et al., *supra* note 75, at 178.

[77] *Id.* at 179.

[78] *Id.* at 180.

[79] *Id.*

[80] *About NIST*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/about-nist (last updated June 14, 2017).

[81] *Id.*

[82] *Work with NIST*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/about-nist/work-nist (last updated Sept. 26, 2017).

The consumer benefit to these standards is simple: the consumer gains devices that can better communicate and work with each other.[83] This interoperability between devices allows consumers to be able to choose from a wide variety of products without having to sacrifice function.[84] Additionally, it influences companies to make better products because they have more competition from each other.[85]

The use of standards also helps to promote security for consumers when using technology that implements those standards.[86] When the industry came together to develop the WiFi standard, they took into account the security concerns inherent in the standard.[87] This led to a more secure system because every company that implemented that technology followed the security standards which were laid out.[88]

E. How Differing Laws Affect the Industry

When technology has widely accepted standards, regardless of where the technology is used, the entire industry applies those standards uniformly to achieve the benefits of the standards.[89] The question then becomes, what happens when different jurisdictions decide to adopt varying standards and regulations? One example of this scenario can be found in the Google Arts & Culture app's "find-your-lookalike" feature released in December of 2017.[90]

This feature allowed users to find their own "art doppelgangers," pieces of art that looked similar to them.[91] The feature works by taking a user's "selfie" and attempting to match it to one of 1,200 artworks in its database using a machine learning algorithm that analyzes the user's face and head position.[92] The feature then shows an image of the art and the user with a percentage indicating how well they matched together.[93]

However, the feature was not made available in Texas and Illinois.[94] At the time of this writing, Google has not yet stated why the feature is not

[83] Biddle et al., *supra* note 75, at 181.

[84] *See id.* (fostering standards, one of NIST's primary responsibilities, gives consumers the ability to choose between multiple products which all likely function on many of the same platforms or use the same technology, e.g. USB).

[85] *See id.* (providing information on NIST funding opportunities, which includes prize competitions and challenges to encourage advancement through competition).

[86] *See generally* Alan Cohen, *Why Standards Are Important for Wireless Security*, SC MEDIA (Feb. 7, 2005), https://www.scmagazine.com/why-standards-are-important-for-wireless-security/article/550011 (describing how standards helped to improve security in WiFi technology).

[87] *Id.*

[88] *Id.*

[89] Biddle, *supra* note 75, at 178.

[90] *See* Hamza Shaban, *A Google App That Matches Your Face to Artworks is Wildly Popular. It's Also Raising Privacy Concerns.*, WASH. POST (Jan. 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/01/16/google-app-that-matches-your-face-to-artwork-is-wildly-popular-its-also-raising-privacy-concerns/?utm_term=.32716bd7456b (describing the Google Art & Culture app's new feature for finding art pieces that look like the user).

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

accessible in Illinois and Texas, but it is suspected that this is because both states have Biometric Information Privacy laws.[95] Users in Illinois have still been able to use the feature while they are present in other states, although they are unable to access the images once they return to Illinois.[96]

Clearly, the difference in laws between the states force technology companies to change how their applications are used depending on where they are. Additionally, the workaround of accessing the data in other states can pose other problems, for example: a consumer may use the feature in neighboring Indiana, then later find a reason to sue Google for an unauthorized use of their data under the Illinois BIPA.[97]

III. ANALYSIS

A. Workarounds and Tricks to Fool a Smartphone's Biometric Authentication Mechanisms

The probabilities of successfully logging in using biometric data compared to a traditional passcode can be vastly different.[98] For example, Apple claims the chances its "Touch ID" will generate a false positive are 1 in 50,000, compared with the chance of guessing a correct 4-digit PIN being roughly 1 in 10,000.[99] It should also be noted that merely adding another digit to a PIN would lower that probability to 1 in 100,000.[100] However, these numbers don't tell the whole story; certain common PIN combinations can offer a higher chance of breaking in.[101] For example, guessing "1234" for a device's PIN code will give roughly a four percent chance of success because that combination is so commonly used.[102] Of course, a full fingerprint is much different than a four-digit PIN, because they are almost completely unique between individuals; however, there are certain patterns of partial fingerprints that are common.[103]

[95] Ally Marotti, *Google's Art Selfies Aren't Available in Illinois. Here's Why.*, CHI. TRIBUNE (Jan. 17, 2018, 7:00 AM), http://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html (providing a potential explanation for why the Google Art & Culture app's new feature is not available in Illinois).

[96] *Id.*

[97] *See* Will Oremus, *Beware of Tech Companies Bearing Privacy Laws*, SLATE (Aug. 28, 2018, 5:50 AM), https://slate.com/technology/2018/08/facebook-and-googles-plan-for-a-new-federal-privacy-law-is-really-about-protecting-themselves.html (noting that the passing of a strict California law is likely to lead to other states to pass laws, some of them much weaker).

[98] Aditi Roy et al., *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems*, 12 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SEC. 2013, 2014–15 (2017).

[99] *Id.*; *About Touch ID Advance Security Technology*, APPLE, https://support.apple.com/en-us/HT204587 (last visited Oct. 20, 2018).

[100] This can be determined by simple math; the odds of guessing 4 digits correctly out of 10 possible digits are calculated by multiplying the odds of guessing each digit, 1/10, by itself 4 times (1/10*1/10*1/10*1/10), which gives a 1 in 10,000 chance. Using the same method the odds for guessing 5 digits would be 1 in 100,000 chance. *See* Probability of Events, MATH PLANET, https://www.mathplanet.com/education/pre-algebra/probability-and-statistic/probability-of-events (last visited Oct. 20, 2018) (explaining how to determine the probability of events).

[101] Roy et al., *supra* note 98, at 2014.

[102] *Id.* at 2015.

[103] *Id.*

Focusing on these partial fingerprint patterns is extremely important because smartphones and devices generally use partial fingerprints rather than a full fingerprint to determine if there is a match.[104] The main reasons for this are the size of the fingerprint sensors themselves and the ability to provide faster access as a result.[105] For example, Apple's fingerprint scanner covers a space of 0.3 inches by 0.3 inches, while the average fingerprint size is 0.5 inches by 0.7 inches.[106] Because only a partial fingerprint is available for comparison the phone records more than one image of the fingerprint so it can have the full picture.[107] When the fingerprint scanner scans your fingerprint it compares it to all of the fingerprint images it has, and if there is a single match access is granted.[108] As a result, if the consumer decides to register more than one finger they may increase the chances of generating a false positive from a partial fingerprint.[109] Apple is not alone in collecting multiple partial fingerprints, Samsung and other phone manufacturers also perform similar methods for collecting fingerprint data from their consumers.[110]

The question then becomes: are there certain common partial fingerprint patterns that can give a potential bad actor access, like the common PIN numbers? The answer, it seems, is that there are common patterns found in fingerprints, and in one study five common patterns were used to generate a positive match about twenty-six percent of the time for one fingerprint matching algorithm, and about sixty-five percent of the time for a separate fingerprint matching algorithm.[111] The study also noted that for cases where multiple fingers were registered on a device the risk would be greater, because generally only one positive match is required.[112]

Finding and using common fingerprint patterns aren't the only way a potential bad actor can exploit the fingerprint scanner and take control of a device. One such method is to use a high resolution image of a person's fingers to create a false fingerprint.[113] This likely won't affect most consumers, as not many people take high resolution pictures of their fingers, but it could pose a threat to high-profile victims, especially if they are photographed frequently.[114] Researchers have also found a way to trick fingerprint sensors in the Samsung Galaxy S6 and Huawei Honor 7 with a normal inkjet printer, special paper, and

[104] *Id.* at 2014.

[105] *Id.*

[106] *Id.*

[107] Goel, *supra* note 12, at 1 (describing several security concerns present in the use of fingerprint sensors as an authentication method).

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] Roy et al., *supra* note 98, at 2023. The study authors do note that the matching algorithm is not the same as the one used by Apple, however the principle is still applicable.

[112] *Id.* at 2023, 2025–26.

[113] *See* Maya Kosoff, *A Hacker Reveals How Your Fingerprint Could Be Easier To Hack Than A Traditional Password*, BUS. INSIDER (Jan. 7, 2015, 2:12 PM), http://www.businessinsider.com/biometric-fingerprint-password-hacking-2015-1 (describing how a fingerprint can be less secure than a traditional passcode).

[114] *Id.*

conductive ink.[115] This method does require a high-resolution image or scan of the finger, while it may not directly affect consumers it could allow law enforcement or other agencies or private companies to gain access if they already have this image.[116] Special tools are not even required in some cases, as shown when a security firm was able to gain access to an iPhone using a fingerprint made from play-doh.[117]

Other popular Biometric Authentication Systems have been fooled as well. The Samsung Galaxy S8's built-in iris scanner was fooled less than a month after it came onto the market.[118] The vulnerability was discovered by a German hacker group who printed an image of the iris, which was taken by a camera in "night-mode," and placed a contact lens on top of the image to mimic the curvature of the eye.[119] Scanning the image with the contact lens granted access to the phone.[120] This was not the only vulnerability in the Galaxy S8, as its facial recognition feature was defeated by a picture displayed on another phone.[121]

Apple's Face ID system has proven much harder to defeat than the Galaxy S8's facial recognition feature and other face authentication methods.[122] At the time of this writing, only one group has managed to successfully defeat Face ID, a Vietnamese cybersecurity firm called Bkav.[123] They managed to defeat the system by creating a mask, although it took weeks to build and had to be positioned carefully.[124] According to the researchers this is more of a concern for high-profile people, as there is much more incentive in creating and working on this sort of mask than there would be for anyone else.[125] Bkav found another "simpler" method to trick Apple's Face ID system later that same month.[126] This

[115] *See* Samuel Gibbs, *Samsung and Huawei Fingerprint Scanners Can be Fooled Using an Inkjet Printer*, THE GUARDIAN (Mar. 8, 2016, 5:50 PM), https://www.theguardian.com/technology/2016/mar/08/samsung-and-huawei-fingerprint-scanners-can-be-fooled-using-an-inkjet-printer (describing a potential flaw in the design of some fingerprint scanners).

[116] *Id.*

[117] *See* April Glaser, *Biometrics are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns (describing potential security concerns associated with Biometric Authentication).

[118] *See* Alex Hern, *Samsung Galaxy S8 Iris Scanner Fooled by German Hackers*, THE GUARDIAN (May 23, 2017, 10:21 AM), https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security (describing a workaround for the Samsung Galaxy S8 iris scanner).

[119] *Id.*

[120] *Id.*

[121] *See* Ron Amadeo, *Galaxy S8 Face Recognition Already Defeated with a Simple Picture*, ARSTECHNIC (Mar. 31, 2017, 10:30 AM), https://arstechnica.com/gadgets/2017/03/video-shows-galaxy-s8-face-recognition-can-be-defeated-with-a-picture (describing how the Samsung Galaxy S8's facial recognition can be fooled to allow a bad actor to gain access).

[122] *See* Andy Greenberg, *We Tried Really Hard to Beat Face ID—And Failed (So Far)*, WIRED (Nov. 3, 2017, 7:00 AM), https://www.wired.com/story/tried-to-beat-face-id-and-failed-so-far (describing potential methods to trick the iPhone X's new Face ID feature).

[123] *See* Mai Nguyen, *Vietnamese Researcher Shows iPhone X face ID 'hack'*, REUTERS (Nov. 14, 2017, 7:46 AM), https://www.reuters.com/article/us-apple-vietnam-hack/vietnamese-researcher-shows-iphone-x-face-id-hack-idUSKBN1DE1TH (describing a method to fool the iPhone X's Face ID feature).

[124] *Id.*

[125] *Id.*

[126] *See* Jack Morse, *Face ID has been Defeated Again, and This Time it was 'Simple'*, MASHABLE (Nov. 27, 2017), https://mashable.com/2017/11/27/apple-face-id-mask-defeated-again/#iAjPjZ0.eiq3 (describing yet another method to fool the iPhone X's Face ID feature).

method utilizes a mask made out of stone powder.[127] This mask gave researches access on their first try, and could be created with only a few photos from different angles.[128]

Apple's support website claims that the feature was designed to work against measures like masks and high-resolution photos, claiming there is only a 1 in 1,000,000 chance that Face ID would be fooled.[129] However, Apple notes that the likelihood of a false match does increase for twins, siblings, and children under the age of thirteen.[130]

B. How Biometric Authentication is Used for Financial Applications

As Biometric Authentication systems became more widespread, financial services began using this as a method to make transactions using smartphones.[131] Financial data can be accessed easily by scanning your fingerprint, rather than entering your username and password.[132] After Apple Pay, Samsung Pay, and Android Pay began using Biometric Authentication methods to make purchases and consumers began to trust those methods, financial institutions followed suit.[133] And of course, both the Google Play Store and Apple App Store allow consumers to make purchases by scanning their fingers, rather than inputting a password.[134]

Now that just about everyone has a smartphone with Biometric Authentication capabilities, banks are increasingly implementing different Biometric Authentication tools for consumers to log in.[135] Bank of America, JPMorgan Chase, and Wells Fargo have all implemented tools for consumers to log into their accounts using the fingerprint scanner on their phones.[136] Wells Fargo has also implemented iris scanning technology to allow consumers to access their accounts.[137] Additionally, MasterCard has developed a tool that allows their customers to log in with a "selfie" and a fingerprint.[138]

[127] *Id.*

[128] *Id.*

[129] *See About Face ID Advanced Technology*, APPLE (Oct. 5, 2018), https://support.apple.com/en-us/HT208108 (describing Apple's new Face ID technology).

[130] *Id.*

[131] Yeap, *supra* note 13.

[132] *Id.*

[133] *Id.*

[134] *See generally Require a Password or Authentication for Purchases*, GOOGLE, https://support.google.com/googleplay/answer/1626831?hl=en (last visited Oct. 21, 2018) (describing how to enable the use of fingerprints for making purchases in the Google Play Store); *see also Use Touch ID on iPhone and iPad*, APPLE, https://support.apple.com/en-us/HT201371 (last visited Oct. 21, 2018) (describing how to enable the use of fingerprints to make purchases on the Apple App Store).

[135] *See* Michael Corkery, *Goodbye, Password. Banks Opt to Scan Fingers and Faces Instead*, N.Y. TIMES (June 21, 2016), https://www.nytimes.com/2016/06/22/business/dealbook/goodbye-password-banks-opt-to-scan-fingers-and-faces-instead.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=Marginalia&pgtype=article (describing the widespread adoption of Biometric Authentication methods by several major Banks).

[136] *Id.*

[137] *Id.*

[138] *See* Luke Graham, *MasterCard Customers Will Soon Be Able to Use a 'Selfie' Password*, NBC NEWS (Feb. 24, 2016, 10:36 AM), https://www.nbcnews.com/business/consumer/mastercard-customers-will-soon-be-able-use-selfie-password-n524921 (describing MasterCard's new selfie password feature).

Not surprisingly, there are currently no laws or regulations that deal specifically with a financial institution's storage or use of Biometric Information.[139] The most relevant law which deals with this information is the Gramm-Leach Bliley Act, which addresses the privacy of personally identifiable financial and account data.[140] The Gramm-Leach Bliley Act's privacy rules relate to financial institutions and their use of "nonpublic personal information."[141] Nonpublic personal information covers personally identifiable financial information: that the consumer provides to the financial institution, where the information resulted from any transaction with the consumer or any service performed for the consumer, or that is otherwise obtained by the financial institution.[142] The Gramm-Leach Bliley Act does not, however, provide guidelines for obtaining that information, nor does it provide guidelines for using that information to authenticate the identity of the consumer.[143]

C. The Adequacy of the Laws on the Books to Protect Consumers

Current laws, like the Illinois BIPA, only provide for protection of the data itself, specifically the retention, collection, disclosure, and destruction processes.[144] The Illinois BIPA requires a private entity in possession of Biometric Information to create a written policy, which must be made available to the public, which establishes a retention schedule and destruction policy that the entity will follow regarding Biometric Information.[145] Further, it prohibits a private entity from obtaining a person's Biometric Information without informing the person of the acquisition of the information, the purpose and term of retention for the information, and without first receiving a release from the person.[146] The Act also prohibits a private entity from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing]" from a person's Biometric Information.[147]

A private entity is also prohibited from disclosing Biometric Information unless: the person has consented to it, the disclosure completes a financial transaction that the person initiated, the disclosure is due to state or federal law or municipal ordinance, or the disclosure is required by a warrant or subpoena.[148] Finally, a private entity must store, protect, and transmit that data according to the standards in the industry, and in the same, or a more secure, manner as the entity stores other confidential information.[149] The Illinois BIPA also provides a right of action for consumers against a private entity that violates the act.[150] Finally, the Illinois BIPA does not apply to any private entity that is included

[139] Claypool & Stoll, *supra* note 10.
[140] *Id.*
[141] *Id.*
[142] 15 U.S.C. § 6809(4)(a) (2018).
[143] Claypool & Stoll, *supra* note 10.
[144] 740 ILL. COMP. STAT. 14/5(g) (2017).
[145] 740 ILL. COMP. STAT. 14/15(a) (2017).
[146] 740 ILL. COMP. STAT. 14/15(b) (2017).
[147] 740 ILL. COMP. STAT. 14/15(c) (2017).
[148] 740 ILL. COMP. STAT. 14/15(d) (2017).
[149] 740 ILL. COMP. STAT. 14/15(e) (2017).
[150] 740 ILL. COMP. STAT. 14/20 (2017).

under Title V of the Gramm-Leach Bliley Act, which mostly covers banks and other financial institutions.[151]

Texas and Washington have also passed similar laws, although neither include a civil right of action for the consumer.[152] Under both the Texas and Washington laws the Attorney General is the one who must bring the civil action against private entities that violate the law.[153] However, both the Texas and Washington laws state their purpose to be similar to the Illinois BIPA, in that they are meant to regulate the retention, collection, disclosure, and destruction process of Biometric Information.[154]

While these laws protect the storage and procurement of a Consumer's Biometric Information, they make no mention of how to securely use that information to protect the consumer from fraud.[155] The only mention made regarding the use of Biometric data is of selling, leasing, trading, or profiting from the data.[156] Therefore, these laws on their own do not create an adequate standard to securely protect consumers' personal devices in the wake of Biometric Authentication.

However, there is still the case law to consider, although case law that applies to the Illinois BIPA is relatively sparse, with the first usage of the law occurring in 2015.[157] Additionally, many of the cases applying the Illinois BIPA are at the federal level, and these cases generally cover three different issues: the application of the law to the information obtained, extraterritoriality, and actual damages.[158] Two cases were decided in the Seventh Circuit's District Courts within months of each other in 2017, *Monroy v. Shutterfly, Inc.* and *Rivera v. Google, Inc.*, which detail each of these issues.[159]

In *Monroy*, the plaintiff alleges that his photograph was uploaded to Shutterfly's database, where Shutterfly analyzed his facial geometry, and subsequently used this biometric data to identify him in other pictures without his consent.[160] Shutterfly argued that they only received the plaintiff's photograph and created the biometric data from that photograph, so they did not violate the BIPA because they did not scan his face geometry in person.[161] The

[151] 740 ILL. COMP. STAT. 14/25(c) (2017).

[152] *See* TEX. BUS. & COM. CODE § 503.001 (providing guidelines similar to the Illinois BIPA); H.B. 1493, 2017 Reg. Sess. (Wash. 2017) (providing a recently passed bill in Washington similar to the Illinois BIPA).

[153] TEX. BUS. & COM. CODE § 503.001(d); WASH. REV. CODE § 19.375.030 (2017).

[154] TEX. BUS. & COM. CODE § 503.001; WASH. REV. CODE § 19.375.020 (2017).

[155] 740 ILL. COMP. STAT. 14/15(c) (2017); TEX. BUS. & COM. CODE § 503.001(c)(1); WASH. REV. CODE § 19.375.020(3).

[156] 740 ILL. COMP. STAT. 14/15(c) (2017); TEX. BUS. & COM. CODE § 503.001(c)(1); WASH. REV. CODE § 19.375.020(3).

[157] *See* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015) (stating that the court could not find any case law interpreting the Illinois BIPA).

[158] *See* Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1092 (N.D. Ill. 2017) (determining if two users of Google's Google Photos application could sue Google under the Illinois BIPA); Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *5 (N.D. Ill. Sept. 15, 2017) (determining whether a non-user's complaint against Shutterfly for storing a picture and identifying it as the user's face would be dismissed).

[159] *See also Rivera*, 238 F. Supp. 3d at 1104 (denying Google's motion to dismiss in February of 2017). *See generally Monroy*, 2017 U.S. Dist. LEXIS 149604, at *27 (denying Shutterfly's motion to dismiss in September of 2017).

[160] *Monroy*, 2017 U.S. Dist. LEXIS 149604, at *2–3.

[161] *Id.* at *8–10.

court found that this is not a valid interpretation of the BIPA and that retrieving the biometric information does not have to be "in-person."[162]

In *Rivera*, the plaintiffs alleged that the photographs of themselves were taken by a "Google Droid device" and uploaded to Google Photos, where the photographs were then scanned to create a template of their faces.[163] The templates were then used to identify and collect photographs with their faces in them, and to collect gender, age, race, and location information about them, without their consent.[164]

In *Rivera*, Google also argued that the BIPA does not apply to information obtained by analyzing photographs or from information derived from photographs.[165] The court here also denied Google's arguments for similar reasons as the court in *Monroy*, stating that there was no textual or structural indication to support the argument.[166] Google also argued that because written consent was required for use of the information, it must follow that the user must give the data in-person as well.[167] The court responded that written consent can be given through "click-wrap" contracts, as is already widely done on the internet and with other devices.[168]

Additionally, both Shutterfly and Google argued that utilizing the BIPA in their cases would be an extraterritorial use of the law.[169] Shutterfly argued in *Monroy* that the violation of the BIPA did not happen in Illinois, and if the suit continued it would be an extraterritorial application of the law.[170] However, Monroy argued that the violation occurred in Illinois because the photo was taken in Illinois and was uploaded to the Shutterfly website from an Illinois IP address, he also argued that Shutterfly did not obtain his consent before retrieving his biometric data.[171] The court found that because it was unclear where the scan of Monroy's face geometry took place and where the scan was stored it was too early to determine if this constituted an extraterritorial use of the law.[172]

In *Rivera* Google offered a similar argument to Shutterfly's, stating that because the face scans and did not occur "primarily and substantially" in Illinois this is an extraterritorial application of the BIPA.[173] The court here also determined that it was too early to make a proper determination of whether this was an extraterritorial application and decided to wait until discovery has concluded to make a determination.[174] The court also noted that determining

[162] *Id.* at *10–12.

[163] *Rivera*, 238 F. Supp. 3d at 1091–92.

[164] *Id.* at 1091.

[165] *Id.* at 1092.

[166] *Id.* at 1096–97.

[167] *Id.* at 1097.

[168] *Id.* at 1097–98.

[169] *Id.* at 1100; Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *15–16 (N.D. Ill. Sept. 15, 2017).

[170] *Monroy*, 2017 U.S. Dist. LEXIS 149604, at *15–17.

[171] *Id.* at *16.

[172] *Id.* at *16–17.

[173] *Rivera*, 238 F. Supp. 3d at 1102.

[174] *Id.*

where the lack of consent and the actual scanning of the photos took place were important determinations that needed to be made.[175] However, these facts are not dispositive on their own and must be taken together to determine extraterritoriality.[176]

Whether there were any actual damages was also considered in *Monroy*.[177] There, Shutterfly claimed that Monroy did not allege any actual damages, so the case must be dismissed.[178] The BIPA does allow a plaintiff to recover $1,000.00 for each violation, however this had not been tested yet in the courts.[179] The court concludes that this issue is quite complex, however they need not decide it at the time because the BIPA does not require a showing of actual damages.[180]

Both *Monroy* and *Rivera* deal with obtaining and storing data under the BIPA, however there is also a case that deals somewhat with using Biometric Data for authentication: *McCollough v. Smarte Carte*.[181] In *McCollough*, the plaintiff rented a storage locker in Chicago's Union Station which was locked using a fingerprint reader.[182] McCollough alleged that Smarte Carte does not inform consumers of how long the data is to be stored, and does not receive written consent for the storage and use of their fingerprints, and that this constituted a violation under the BIPA.[183] The court found that this violation of the statute did not create Article III standing, because there was no injury in fact suffered by McCollough, and dismissed the case.[184] The court also noted that the standing requirement would not be present in state court, however even if the state court could find that there was injury in fact as a result, there still could be no standing under Article III.[185]

McCollough is the most similar case to the problem described in this Note, even though it deals with the storage of Biometric Information used for Authentication, rather than the actual *method* of Authentication.[186] However, it would be hard to imagine that there would be an Article III standing issue in a case that deals with Biometric Authentication, as that would likely create an injury due to the breach of data.[187] The more interesting issue here is that of

[175] *Id.*

[176] *Id.*

[177] *Monroy*, 2017 U.S. Dist. LEXIS 149604, at *21.

[178] *Id.* at *21–22.

[179] *Id.* at *22–25.

[180] *Id.* at *26–27.

[181] *See* McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 U.S. Dist. LEXIS 100404 (N.D. Ill. Aug. 1, 2016) (dismissing a case brought against Smarte Carte under the BIPA).

[182] *Id.* at *1–3.

[183] *Id.* at *3.

[184] *Id.* at *12–14.

[185] *Id.* at *13–14.

[186] *See generally id.* (failing to discuss whether collecting the fingerprints was justified).

[187] Consumers do face some challenges when establishing standing after their data has been breached, but this goes beyond the scope of this note. The following cases illustrate the difficulty in acquiring standing in these situations and offer a good starting point for research into this issue. *See generally* Doe v. Chao, 540 U.S. 614 (2004) (noting that the plaintiff needed to show an injury-in-fact to satisfy the Article III even under the claim of the breach of a Social Security Number); Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015) (concluding that an imminent and financial loss can support an injury-in-fact for the Article III standing under the claim of the breach of credit card information).

extraterritoriality, as seen in *Rivera* and *Monroy*.[188] If the courts do decide that the application of the BIPA in either case was extraterritorial, it could be rendered almost useless, as Illinois citizens will likely be unable to seek relief from companies who operate outside of Illinois, but would violate the statute otherwise.[189]

The recent adoption of the General Data Protection Regulation (GDPR) by the European Union is another step taken to create standards and policies for consumer data.[190] This regulation provides consumers with a set of rights regarding the collection and use of their data but fails to include any direction related to the use of personal data for authentication.[191]

D. The Industry's Attempt to Create a Standard

Although no federal or state law currently exists that creates a standard for device companies to follow, the industry has made attempts to create a standard themselves.[192] In a series of talks spanning over 16 months, consumer groups and trade associations convened to discuss privacy concerns with facial recognition and authentication software.[193] These talks were a part of President Obama's efforts to establish a "consumer privacy bill of rights."[194] Unfortunately, this conference did not result in any change or agreement between the consumer groups and the trade associations.[195]

Regardless, both Apple and Google have created their own separate standards for locking and unlocking devices with Biometric Authentication.[196] Apple's standard requires the use of a passcode if: the device has just been turned on, the device hasn't been unlocked for more than forty-eight hours, the passcode hasn't been used in the past six and a half days and Face ID has not unlocked the device in the past four hours, the device was remotely locked, there were five unsuccessful attempts to match a face, or after holding down either volume button and the side button simultaneously.[197] Google's standard is much simpler, and requires the passcode if the fingerprint isn't recognized after a few

[188] *See* Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *15–16 (N.D. Ill. Sept. 15, 2017) (discussing extraterritorial application of the Illinois BIPA); Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017) (discussing extraterritorial application of the Illinois BIPA).

[189] *See, e.g.*, *Rivera*, 238 F. Supp. 3d at 1088 (the Illinois court has not decided on the matter of extraterritoriality).

[190] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (replacing a general data protection regulation with a regulation that more specifically protects the processing and transferring of personal data).

[191] *Id.*

[192] Singer, *supra* note 11.

[193] *Id.*

[194] *Id.*

[195] *Id.*

[196] *See generally Face ID Security*, APPLE, INC. (Nov. 2017) [hereinafter *Face ID Security*], https://images.apple.com/business/docs/ FaceID_Security_Guide.pdf (describing Apple's standards for the use of Face ID as Biometric Authentication); *Unlock with Your Fingerprint*, *supra* note 6 (describing Google's standards for the use of a fingerprint as Biometric Authentication in the Google Pixel).

[197] *Face ID Security*, *supra* note 196.

attempts, the phone has restarted, the phone is switched to a different user, or more than 48 hours have passed since unlocking with the backup PIN.[198]

E. An Industry-Wide Standard Can Help to Alleviate these Issues

As seen with Google Arts & Culture's "find-your-lookalike" feature, differing state laws can prompt companies to release technology that only works when in a certain geographic area.[199] This creates a different experience for users based merely on their geographic location, and is contrary to one of the reasons we have standards in the first place: to provide uniformity and security to users.[200] Because the Texas and Washington Biometric Information Privacy laws closely resemble Illinois' BIPA,[201] I will analyze this feature in the context of the Illinois BIPA.

The first requirement of the Illinois BIPA is that the company must develop a written policy documenting and establishing a retention schedule and guidelines for permanently destroying the Biometric Identifiers and Information when the purpose for collecting the data has been satisfied, or within 3 years.[202]

The Google Arts & Culture app uses Google's standard privacy policy, which will be used for this analysis. [203] Google's Privacy Policy provides that they may collect a user's name and photo.[204] Google also states that it uses this information to "to provide, maintain, protect and improve [the data], to develop new [data], and to protect Google and our users."[205] However, Google does not provide any information about data retention, nor does it provide any guidelines for destroying this data.[206]

Google's Patrick Lenihan has stated that Google is not using the selfies for anything other than art matches.[207] Additionally, the app itself states that the photos are only stored until a match is found.[208] However, these statements are not enough, as the BIPA requires this information to be stated in a written policy, and language similar to Mr. Lenihan's and the information provided in the app

[198] *Unlock with Your Fingerprint*, *supra* note 6 (describing how to set up fingerprint authentication for Google's phones).

[199] Shaban, *supra* note 90.

[200] Biddle et al., *supra* note 75, at 178.

[201] TEX. BUS. & COM. CODE § 503.001; H.B. 1493, 2017 Reg. Sess. (Wash. 2017) (a recently passed bill in Washington similar to the Illinois BIPA).

[202] 740 ILL. COMP. STAT. 14/15(a) (2017).

[203] *See Google Arts & Culture*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.google.android.apps.cultural&hl=en (last visited Oct. 22, 2018) (noting that the privacy policy can be accessed by scrolling down to the bottom of the app description and clicking Privacy Policy under the "Developer" Heading).

[204] *Google Privacy & Terms*, GOOGLE, https://www.google.com/policies/privacy (last visited Oct. 21, 2018).

[205] *Id.*

[206] *See id.* (describing Google's privacy policy but providing no information on how Biometric Data or Information is destroyed after its use is no longer needed).

[207] Shaban *supra* note 90.

[208] *Id.*

is not documented in Google's Privacy Policy.[209] As is clear, Google's privacy policy does not comply with even the first requirement of the Illinois BIPA.[210]

This provides evidence of how the different laws and standards affect consumers and businesses.[211] The effect on the issue of providing a standard for the use of Biometric Authentication in our smartphones and personal devices seems clear: if one jurisdiction decides to adopt a policy, it can be bypassed by going to another jurisdiction without those protections, as seen with the Google Arts & Culture App.[212] However, if the industry as a whole or a federal regulatory body adopts a standard on the use of Biometric Authentication it may be enough to prompt technology manufacturers to adopt the standard universally, and alleviate this issue.[213]

IV. RECOMMENDATION

Both Apple and Google's standards provide more security than Biometric Authentication alone, as they require a passcode that only the consumer would know if the scanners do not detect a match, or if the phone has been out of the consumer's possession for too long.[214] However, a recent poll shows that, on average, Americans look at their phones 47 times per day (about twice per hour).[215] At that rate, if a device is stolen it seems more likely than not that the thief has about forty hours to determine how to unlock the phone and access personal and financial data.[216]

Because of the myriad of techniques that can be used to unlock a phone protected by Biometric Authentication, it is likely that the information stored on our phones is at great risk if the phone itself is stolen.[217] In addition to the information stored on the smartphones, access to various financial services could also be gained in this timeframe.[218] Additionally, because most companies have

[209] *Google Privacy & Terms*, *supra* note 204.

[210] *See* 740 ILL. COMP. STAT. 14/15 (2017) ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public . . . .").

[211] Maroti, *supra* note 95.

[212] *Id.*

[213] *See, e.g.*, FIDO ALLIANCE, https://fidoalliance.org (last visited Oct. 21, 2018) (providing an example of an organization that advocates for universal authentication standards).

[214] *See generally Face ID Security*, *supra* note 196 (describing Apple's standards for the use of Face ID as Biometric Authentication); *see also* Unlock With Your Fingerprint, *supra* note 6 (describing Google's standards for the use of a fingerprint as Biometric Authentication in the Google Pixel).

[215] *2017 Global Mobile Consumer Survey: US Edition*, DELOITTE [hereinafter *Mobile Consumer Survey*], https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html (last visited Oct. 21, 2012).

[216] Vindu Goel, *The Fingerprint Sensor on Your Phone Is Not as Safe as You Think*, N.Y. TIMES (Apr. 10, 2017), https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html.

[217] *See generally* Calla Deitrick, *Smartphone Thefts Drop as Kill Switch Usage Grows: But Android Users are Still Waiting for the Technology*, CONSUMER REP. (June 11, 2015), https://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm (showing the large number of smart phones that are stolen each year, and the security risks inherent in certain devices that cannot be remotely wiped to protect its owner's data).

[218] *See generally* Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015 (showing that 57% of smartphone users have used their phone to do online banking).

different standards regarding how often the phone requires a passcode, and because there are no universal standards, laws, or regulations, in some cases there can be even more time for a criminal to gain access to your smartphone or device.[219]

A. Minimum Standards for Financial Applications

A first step is to create established minimum standards for authentication for financial applications or making purchases. For the most part, once a criminal has tricked the phone's Biometric Authorization mechanism they will have access to financial accounts which use the same mechanism, as well as the ability to make purchases using the phone if Apple Pay, Google Pay, or a similar application is configured.[220] Essentially, using the Biometric Authentication alone is not enough to protect consumers from fraud through the use of their financial applications, and it should be required, at minimum, for those applications to ask for a two-factor authentication, consisting of the Biometric method and a PIN or password.[221]

The addition of a second factor for the user to provide obviously flies in the face of the ease of use Biometric Authentication provides, providing two pieces of information is inherently harder than providing only one after all.[222] However, preventing fraudulent charges and changes to a user's financial accounts in the scenario that a thief is able to unlock a phone should be a powerful enough incentive to counter this minor inconvenience.

At the very least, this two-factor authentication should be required after a certain number of uses of the financial application have occurred, a number of unsuccessful attempts to access the application occur, or when performing certain actions like a transfer of funds in order to minimize damage as much as possible. This would provide more protection for the users than is currently available.[223]

B. Standard Practices for a Device's Biometric Authentication Mechanisms

My next proposal is establishing standard practices for inputting a non-biometric password in other circumstances. These would be based on certain events, for example: if the passcode hasn't been entered after a certain amount of time or when the device is restarted. Both Apple and Google already implement some of these practices already, however creating a minimum

[219] As already shown, Apple and Google already have different policies in place, and it would not be a stretch of the imagination to assume that other companies would have different policies as well.

[220] *See generally Back to Basics: Multi-Factor Authentication (MFA)*, NIST, https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication (last updated Nov. 22, 2016) (describing Multi-Factor Authentication).

[221] *Id.* Two-factor, or multi-factor, authentication, describes the use of more than one authentication method for the purposes of security. This can be as simple as requiring a password and a pin code and can lower the risk of a bad actor accessing an account. For example: there is a 1 in 10,000 chance of someone correctly guessing a four-digit PIN and Apple claims there is only a 1 in 50,000 chance of another person accessing a device using TouchID; however, if both a correct fingerprint and PIN are required the chance of a bad actor accessing the device falls down to 1 in 500,00,000.

[222] *See id.* (explaining the process of two factor authentication).

[223] *Id.*

standard for all manufacturers to follow is necessary because smaller companies may not have standards nearly as strict as Apple and Google.[224]

Additionally, in light of the fact that on average we look at our phones forty-seven times per day,[225] or slightly under twice per hour, a minimum forty-eight hour window, like that used by Google and Apple, is clearly too long.[226] Shortening the window would be preferable because it would allow a potential criminal less time to gain access while still ensuring that the speed benefit for Biometric Authentication is preserved.[227] I would recommend shortening this interval to eight hours, as it likely will not give a criminal enough time to create the necessary tools, like fake fingerprints or a high quality photo or model of the consumer's face, to obtain access to the device.[228] It will also still be long enough for a consumer to be able to frequently unlock their device without having to enter their passcode, because they will only need to do so a maximum of three times per day.

In order to preserve consumers' desire for ease of access these minimum standards can also include identifying safe areas where only single-factor authentication, through the Biometric Authentication, is required. This would be implemented by giving the user the option to identify safe areas and requiring them to use a two-factor authentication method when their device is not in one of those locations. This will still prevent bad actors from stealing sensitive information, because it is not likely that they would steal a device and try to access it in one of the defined safe areas, as this would increase the risk that the device's owner would be able to catch them in the act.[229] A similar technology already exists for Android-based devices that automatically unlocks the device based on where it is.[230] It would likely not be difficult to repurpose this technology to be used with Biometric Authentication.[231]

It may also be beneficial if device manufacturers used a full fingerprint, rather than a partial fingerprint.[232] This would negate the false matches that can result when using partial fingerprints, and create a more secure system.[233] A full fingerprint may require larger fingerprint scanners or a different method of

[224] *See* Kelsie Anderson, *How Multi-Factor Authentication Options Keep Small Businesses Secure*, GETAPP LAB (Dec. 21, 2017), https://lab.getapp.com/how-multi-factor-authentication-options-keep-small-businesses-secure (discussing how nearly half of cyber-attacks target small businesses).

[225] *Mobile Consumer Survey*, *supra* note 215.

[226] *See About Touch ID Advanced Security Technology*, APPLE, https://support.apple.com/en-us/HT204587 (last visited Oct. 21, 2018) (explains how a phone user must enter a password when more than 48 hours have passed).

[227] *See Unlock with Your Fingerprint*, *supra* note 6 (showing the relatively fast nature of biometric authentication standard methods); *Use TouchID*, *supra* note 6 (similarly illustrating the relatively fast nature of biometric authentication standard methods).

[228] *See supra* Part III.A (explaining the workarounds used to circumvent biometric authentication).

[229] *See generally Set Your Device to Automatically Unlock*, GOOGLE, https://support.google.com/nexus/answer/6093922?hl=en (last visited Oct. 21, 2018) (showing an example of a technology that utilizes the safe-area unlocking feature).

[230] *See id.* (describing how to set the Google Nexus to automatically unlock when in a certain location).

[231] *Id.*

[232] Suruchi Devanahalli, *Security Vulnerabilities of Apple iPhone Fingerprint Authentication*, TUFTS DEP'T COMP. SCI. (2017), http://www.cs.tufts.edu/comp/116/archive/fall2017/sdevanahalli.pdf.

[233] *See* Roy et al., *supra* note 98, at 2014–15 (describing the drawbacks in using partial fingerprints for Biometric Authentication).

scanning fingerprints than is currently used, which may be slower than the current method.[234] However, because of the rate that computing power grows, this will not be a problem for very long.[235]

C. The Industry as a Whole, or the Federal Government, Should Create a Uniform Standard

A uniform standard must be established on the federal level, through NIST, or industry-wide. If it is not, there will be too many jurisdictions with differing requirements, which will only cause confusion and defeat the purpose of having such a standard.[236] As a result, we will only have a repeat of the same problem faced by Google's Arts & Culture app.

One of the risks that will follow if a universal standard is not created is that device manufacturers will check a device's location and apply different standards, depending on where it is.[237] This would create a risk that potential bad actors will take a device to another jurisdiction with more lax standards and be able to access that device's information there.[238] In another scenario, only consumers in certain jurisdictions will be able to enjoy the benefit of the increased security that a Biometric Authentication standard or law will provide, consequently leaving consumers in other jurisdictions vulnerable.[239]

These risks have already been illustrated by the situation surrounding Google's Arts & Culture app.[240] Google limited the release of the app's new feature based on the location of the user's phone.[241] This resulted in a consumer's relatively easy ability to bypass the restriction by simply travelling across their state's border to another state.[242] Obviously a smartphone thief will be able to easily travel across state lines to any other state with relaxed Biometric Authentication security standards within the 48 hour window described in Google's and Apple's standards.[243] Additionally, for Android-based devices, with the widespread availability of "location-spoofing" applications, travel to another state may not be necessary at all.[244] Further, under Google's standard, all a thief needs to do is keep the phone on and frequently enter the passcode to

[234] *Id.*

[235] *See* Clark, *supra* note 26 (describing "Moore's Law" and the rate of growth of computing power over time).

[236] *See generally* Marotti, *supra* note 95 (explaining why, for example, the Google Arts & Culture app is unavailable in Illinois).

[237] *Id.*

[238] *Id.*

[239] *Id.*

[240] *Id.*

[241] *Id.*

[242] *Id.*

[243] A flight from Maine to Hawaii, two states on the opposite sides of the United States would be just under 11 Hours, leaving at least 30 hours for the thief to take the required actions to unlock the device. TRAVELMATH, https://www.travelmath.com/flying-time/from/Portland,+ME/to/Honolulu,+HI (last visited Oct. 21, 2018); *see Face ID Security*, *supra* note 196 (stating that a passcode is required when the device has not been unlocked for 48 hours).

[244] Chris P., *Here's How to Easily Fake Your GPS Location on Android*, PHONEARENA (July 1l, 2016), https://www.phonearena.com/news/Heres-how-to-easily-fake-your-GPS-location-on-Android_id62775 (describing how to fake a location in Android Phones).

retain access.[245] For Apple products, thieves can only do this for a little less than a week; however, that is more than enough time to retrieve data and wreak havoc on a user's financial accounts.[246]

Of course, it is possible that device and smartphone manufacturers will opt to simply follow the strictest security standard in order to maintain consumer confidence, and because it would be much easier to implement the same standard in all of their products.[247] Currently, the only example of differing uses of Biometric Information based on a user's location is the Arts & Culture app situation, which evidences that changing the security standards for Biometric Authentication based on the user's location is more likely.[248] However, as the *Rivera* and *Monroy* cases show, there are additional issues with extraterritoriality when applying laws from other states that may render the laws created useless, unless they are uniform or universal in some way.[249] Additionally, these varying standards could cause confusion and an even less secure system, as the use of many variable standards go against the reason technology companies create standards to begin with.[250] Not to mention the fact that the varying security standards could create a larger burden on smaller device manufacturers and give an unfair advantage to Apple and Google, whose infrastructure renders them better adaptable to differing laws.[251]

V. CONCLUSION

As Biometric Authentication technology evolves, it becomes increasingly clear that there is a need for standards which provide device security.[252] Technology will advance, and as it does, new methods of defeating these systems will emerge.[253] There are currently no industry standards to ensure stronger security for smartphone Biometric Authentication, and the existing laws are not well-equipped to fill this gap.[254] In fact, the existing laws may not even apply as they are intended due to issues like extraterritoriality and assessing whether there is an injury-in-fact.[255] Creating a minimum two-factor authentication for financial services, a uniform standard for inputting a backup PIN frequently, and implementing these proposals on a national level will

[245] *Unlock with Your Fingerprint*, *supra* note 6.

[246] *Face ID Security*, *supra* note 196.

[247] *See supra* Part IV.B (author's proposal of a strict security standard to maintain consumer confidence).

[248] *See generally* Marotti, *supra* note 95 (describing location problems in Illinois for Google's Arts & Culture app).

[249] Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *1, *15–16 (N.D. Ill. Sept. 15, 2017); Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017).

[250] Biddle et al., *supra* note 75.

[251] *Id.*

[252] *See supra* Part IV.C (discussing the need for a standard).

[253] *See* Chris P., *supra* note 244 (describing one method of defeating the 'system').

[254] *See* Claypool & Stoll, *supra* note 10 (providing a brief overview of Biometric Information laws, standards, and regulations).

[255] *See generally* Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *1 (N.D. Ill. Sept. 15, 2017) (assessing extraterritoriality and injury issues); *see also* Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017) (assessing extraterritoriality and injury issues).

greatly improve smartphone security and will be a valuable step in the right direction.[256]

[256] *See supra* Part IV.B (recommending two-factor authentication and a standard to increase phone security).