Putting a Finger on Biometrics Law

by: Amanda Heine

Americans nationwide are walking into their place of employment Monday through Friday and either placing their finger on a scanner, having their face analyzed by a beam or even the iris of their eye digitally scanned. The process of clocking in for work with your fingerprint has become extremely jejune. This process is more often than not required by employers before an employee can start their work day. Whether biometrics is used for logging in hours, authentication, or security purposes, it is typically a 'use it' or 'lose the job' scenario. Though biometrics might be making the workplace increasingly more efficient and innovative, it also comes with new risks. Employers are especially at risk with potential liability encompassed within privacy law and how this data is obtained and stored. The employers require their employees to submit to the use of biometrics, yet there are minimal to zero required obligations owed to the employee by the employer. There are currently no federal regulations put in place for the protection of employee privacy rights relative to biometrics.

Introduction

In an assortment of public and private institutions, biometric technology is becoming a prevalent means to identify individuals. This is due to biometric technology's alleged superior control and efficiency of access to many aspects of identification protocols used by these institutions. The idea of biometrics has been around since the dawn of Star Trek in the 1960's with the concept of voice ID, retina scan and facial recognition. Remember when Captain Kirk of Starship Enterprise would just speak to the ship and the ship would just know who he was? Well, that is biometric technology. Captain Kirk also used biometric

technology to access Project Genesis with the use of a Retina Scan.[1] Just to think about the idea of biometric technology from a 1960s fictional series that has become reality today is phenomenal. Unfortunately the crucial part the movies left out is that these devices need to be programmed. The devices don't "just know" an individual, they have to be queried with a physical attribute that is distinct to a specific individual. What the movies did get right was some of the shortcomings of biometric technology. They portrayed how easy it was to procure a fingerprint from a glass or door handle by the use of wax or tape. That finger print then could be replicated and applied using molds. The intent of this research is to provide main ideas and drivers in the area of biometric technology and privacy to raise awareness to the innovative possibilities and of the foreseeable issues that emerge. The basic usages of biometric modalities has become a conventional method for use in identifying individuals and an efficient technology to support elevated security measures. It is important to note that there are risks associated with the use of biometric identifiers and consideration must be given to the possibility of failed system integrity. Finally, concerns related to constitutional protections along with current and pending legislation must also be considered.

The Basics of Biometrics

There is no ubiquitous definition for biometrics but it is generally referred to as measurable human biological and behavioral characteristics that can be used for identification and/or and automated method(s) of recognizing or analyzing an individual based on human

[1] Project Genesis, StarTrek.com, http://www.startrek.com/database_article/project-genesis, (last visited March 5, 2019.)

biological and behavioral characteristics.[2] Biometrics have been gradually subjugating the usage of passwords and the usage of physical keys. Due to the emergence of these technologies there is an increased necessity to find balance between the safeguard of individual privacy rights and the implementation of advanced technologies.

When we think of Biometrics, we think of the future. But biometrics are not the future anymore, they are the present. This technology has become a favored human identifier due to its perceived reliability and its uniqueness of a "one-to-one" match.[3] Collecting biometric identifiers is now gathered through the use of scans that then analyzes the significant data turning it into an algorithm that can be used to uniquely identify an individual. One of the oldest identifiers used is the fingerprint. The use of ink and paper for biometric identification to reduce forgery has been around since the 1800s. Fingerprints were found on pre-historic clay tablets as seals and a type of signature for business transactions.[4] It was in the 1880's when fingerprints were notably recognized to be a means of distinct personal identification. In 1892, the first fingerprint identification was used to identify a murderer, thereby establishing the significance of fingerprints.[5]

---

[2] Barbara Harris and Susan Sholinsky, *Biometrics in the Workplace,* (June2018), https://www.ebglaw.com/content/uploads/2018/02/Sholinsky-Steinmeyer-Reuters-Expert-QA-Biometrics-February-2018.pdf, (last visited Feb. 28, 2019.)

[3] Lauren D. Adkins, *Biometrics: Weighing Convenience and National Security Against Your Privacy*, 13 Mich. Telecomm & Tech. L. Rev. 541, 2007, http://repository.law.umich.edu/mttir/vol13/iss2/10, (last visited March 5, 2019.)

[4] *The History of Finger Prints*, 2012, https://www.acschools.org/cms/lib/PA01916405/Centricity/Domain/362/The History of FingerprintsUpdated 21 August 2012.pdf., (last visited March 5, 2019.)

[5] Cyril John Polson, *Finger Prints and Finger Printing: An Historical Study*, American Journal of Police Science, 41 J. Crim. L. & Criminology 495 (1950-1951), https://heinonline.org/HOL/LandingPage?handle=hein.journals/jclc41&div=86&id=&page=, (last visited March 5, 2019.)

The use of fingerprints for identification has transformed over the years. We now use scanners rather than clay and ink. Another identifier less commonly used as a biometric modality is hand geometry. Hand geometry uses characteristics such as the length, width, and surface area of the hand to create a map which is then used as the identifier.[6] This means of identification is used less frequently considering its limited accuracy. The use of hand geometry is generally incorporated with other biometric modalities similar to the two-step verification process that is utilized with passwords. Both hand and finger imprinting are more likely to be accepted by the general public as they are less invasive.[7] Facial recognition is becoming more widely used because it is less invasive. Facial recognition has been used for years but in the form of composite sketches for forensic use.[8] Facial recognition has now developed into a process in which technology captures and maps facial features which include the nose, eyes, and mouth. Capture can be accessed by either static photos or video images. One challenge to this modality is that facial appearances tend to change overtime which threatens the authenticity and reliability of the process.[9]

[6]Lauren Adkins, *Biometrics:weighing Convenience and National Security Against Your Privacy*, 13 Mich. Telecom. Tech. L. Rev. 541, 2007, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1096&context=mttlr, (last visited March 5, 2019.)

[7] Id.

[8] Jonghyun Choi et al., *Data Insufficiency in Sketch Versus Photo Face Recognition*, Institute for Advanced Computer Studies, University of Maryland, http://users.umiacs.umd.edu/~jhchoi/paper/cvprw2012_sketch.pdf, (last visited March 5, 2019.)

[9] Id.

Ocular biometrics are another unique way to recognize individuals. These modalities use iris, periocular, retina, and eye movement scans.[10] Retina scan technologies require close contact to map the fine network of capillaries using a low intensity light that is sent through the eye. Challenges with retina scans are created by degenerative disorders of the retina.[11] Voice recognition is developed when a distinct intonation, pitch, and pronunciation of a voice is measured and then compared to a previously stored voice sample.[12] To capture a voice imprint an individual will traditionally recite a verbal or numerical phrase.[13] Voice recognitions can utilize a fixed set of phrases or recognized voice patterns. These systems are not as accurate as fingerprinting or iris scans as an individual's voice can change with health and emotional states.[14]

Some other emerging behavioral characteristics utilized for biometric identification are written signatures, keystroke dynamics and gaits.[15]

---

[10] Ishan Nigam, Mayank Vatsa & Richa Singh, *Ocular biometrics: A survey of modalities and fusion approaches*, 26 Information Fusion, 2015, https://www.semanticscholar.org/paper/Ocular-biometrics%3A-A-survey-of-modalities-and-Nigam-Vatsa/45f4b0087fdcc17f122cc4f7a9aa19dd51b40669, (last visited March 5, 2019.)

[11] *Biometric Eye Scans*, The Columbia Encyclopedia, 6th ed., 2019, https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/biometric-eye-scans, (last visited March 5, 2019.)

[12] Langenderfer, J. and Linnhoff, S., *The Emergence of Biometrics and Its Effect on Consumers*, Journal of Consumer Affairs, 2005, Wiley Library Online, https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2005.00017.x, (last visited March 5, 2019.)

[13] Id.

[14] *Voice Verification*, Global Security, https://www.globalsecurity.org/security/systems/biometrics-voice.htm (last visited March 5, 2019).

[15] Id.

Gait is the manner in which an individual walks. This modality is captured through gait recognition systems. Gait is less accurate than most other biometric identifiers due to environmental factors like walking surfaces and shoe choice. This can cause flawed measurability.[16] Other more intricate interactions that are used in biometrics are hand-eye coordination as well as hand tremors. All of these means of analyzing data create variables that lead to the heightened possibility of error.[17] Biometrics have been gradually subjugating the usage of passwords and the usage of physical keys. Due to the emergence of these technologies, there is a increased necessity to find balance between the safeguard of individual privacy rights and the implementation of advanced technologies.

Efficiency and Risks

The username and password era is becoming a thing of the past in our society. Especially since now you need a twelve character password with one upper case letter, two numbers, and a special character. Then you need multi-factor identification before you can login which will be sent to an email address which requires another twelve character password, with an upper-case letter, two numbers and a special character. That password to your email also needs multi-factor authorization which will send a text of a six digit number to your cell phone. Then you will have to input the digits within 10 seconds to access the email but before you can get those digits you need to use a

[16] Id.

[17] Avi Turgeman, *Behavioral Biometrics Are Not New, So Why Are They So Hot Right Now?* Forbes, 2017, https://www.forbes.com/sites/forbestechcouncil/2017/06/20/behavioral-biometrics-are-not-new-so-why-are-they-so-hot-right-now/#7050997a33d7, (last visited March 5, 2019.)

biometric fingerprint to unlock that phone. After spending about 10 minutes or more trying to login to protected data you ask, "why didn't I just lead with that biometric identifier?" Biometrics fill the need of being able to accurately identify people in a timely manner in order to allow the access and exchange of sensitive data which may include health and financial data. A serious concern is the need to remember all of the different lengthy passwords.

The Department of Homeland security has been using biometric technology to detect and prevent illegal entry into the U.S., grant and administer proper immigration benefits, vetting and credentialing, facilitating legitimate travel and trade, enforcing federal laws, and enabling verification for visa applications to the U.S.[18] In 2013, the Department of Homeland Security replaced the U.S. Visitor and Immigration Status Indicator Technology Program(US- VISIT) with the Office of Biometric Identity Management (OBIM). The OBIM system is assumed to enable national security and public safety decision making.[19] Homeland security released a Privacy Impact Assessment which outlines a few of the privacy risks of the biometric data system.[20] The assessment implies that there is a risk to the quality and integrity of the biometric data collection and management which may cause misidentification. It also suggests that data which is collected by a mobile device is susceptible to monitoring, interception, and tampering by unauthorized individuals. The most harrowing of risks is that the biometric information collected does not correctly map to one

[18] *Biometrics*, Office of Biometric Identity Management, Homeland Security, https://www.dhs.gov/biometrics, (last visited Feb. 28, 2019.)
[19] Office of Biometric Identity Management, Homeland Security, https://www.dhs.gov/obim, (last visited Feb. 28, 2019.)
[20] *Privacy Information.* Office of Biometric Identity Management, Homeland Security, https://www.dhs.gov/obim-privacy-information, (last visited Feb. 28, 2019.)

individual or even worse, it involves collecting data from individuals who are not offenders and the inappropriately collected data is retained inappropriately and indefinitely.[21]

Biometric technology isn't just a password that can be easily changed. It is technology that identifies you by something that is part of you which is immutable. If these identifiers are copied and hacked there is almost no way to change your password unless you change your fingerprint.

The risk for consumer skeptics like Snowden and Matrix fans is that they do not want the government tracking their every move. There is also the risk that there may be technology errors that are not easily corrected or that put people in terrible positions with law enforcement. There is also the concern that the data can be manipulated to indicate that a person was physically present when they weren't. Because this type of data is considered so reliable, there is also the concern that it will not be adequately evaluated and dealt with.

Consumer Considerations

It is recognized that consumers are skeptical of new things especially in a century flooded with telemarketers and spammers.[22] The consumer skeptics who arise with biometric technology are those who are avid

[21] Cantor, J., *Privacy Impact Assessment for the Automated Biometric Identification System,* U.S. Department of Homeland Security, 2012, https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf, (last visited Feb. 28, 2019.)

[22] Kaj P.N. Morel and Ad Th.H. Pruyn, *Consumer Skepticism Toward New Products*, European Advances in Consumer Research, 2003, https://research.utwente.nl/en/publications/consumer-skepticism-toward-new-products, (last visited March 5, 2019.)

Snowden and Matrix believers. They don't want the government tracking their every move, like the program the Department of Homeland Security uses for tracking immigrants. It is programs like this that create dubiousness about biometric modality use. The view of biometric use differs drastically between social groups considering the variation in cultural values and beliefs.[23] One social group may endorse the iris scans when checking into a hospital while the same social group may object to the use of facial recognition when walking into a department store. The intangible interactions between a biometric system and an individual are commonly overlooked. The willingness of an individual to participate and accept biometric use usually relies on the perceived safety and the presumed benefit.[24] Then we must also acknowledge that individual participation is driven by the potential consequences to those who don't participate.[25] If an individual chooses not to use biometrics, then they may not get a job or may be subject to isolation for certain social interactions. Systems must be diverse. And consideration must be given to ADA requirements.[26]

---

[23] Consensus Study Report, *Biometric Recognition: Challenges and Opportunities*, National Research Council (US), Whither Biometrics Committee, 2010, https://www.ncbi.nlm.nih.gov/books/NBK219893/, (last visited March 5, 2019.)

[24] Concensus Study Report, *Who Goes There? Authentication Through the Lens of Privacy*, The National Academies Press 2003, https://www.nap.edu/catalog/10656/who-goes-there-authentication-through-the-lens-of-privacy, (last visited March 5, 2019.)

[25] Lancelot Miltgen, C., Popovič, A. and Oliveira, T., *Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context*, Decision Support Systems, 2013, https://www.researchgate.net/publication/258821079_Determinants_of_end-user_acceptance_of_biometrics_Integrating_the_Big_3_of_technology_acceptance_with_privacy_context, (last visited March 5, 2019.)

[26] Title III, ADA Requirements, 2011, https://www.ada.gov/reg3a.html, (last visited March 5, 2019.)

Certain individuals may not feel they can enroll in these systems as a result of physical inhibitions.[27] It is also important to consider the complications that these systems establish for an individual and their First Amendment rights. Having a mandatory requirement of biometric use begets de facto discrimination.[28] Consumers may also be skeptical about the standards used with biometrics. For instance, with facial recognition software, solitude may no longer be possible.[29] One day the notion of walking outside will no longer be a simple liberty. Things like 3D cameras with automated facial recognition that have been rapidly advancing in technology create foreseeable privacy implications.[30] In this scenario we must acknowledge that there is no real opt-out in a digital age with cameras everywhere. To function in society one must walk outside in public to participate.

When public and private sectors converge their facial recognition databases, do we not expose our faces in public? Many of us have experienced a moment when using Facebook or other means of social media where you receive a prompt to tag someone by name. This feature of tagging someone you may know was developed by the use of software which uses mass collection of facial geometric mapping through photos on various sites. The case of *Licata v. Facebook*, INC.,

---

[27] Id.
[28] Id.
[29] Katherine Strandburg and Daniela Stan Raicu, eds,. *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation,* 2006, *https://www.springer.com/us/book/9780387260501*, (last visited March 5, 2019.).
[30] Jennifer Tucker, *How Facial Recognition Technology Came To Be*, 2014, Globe Correspondent, https://www.bostonglobe.com/ideas/2014/11/23/facial-recognition-technology-goes-way-back/CkWaxzozvFcveQ7kvdLHGI/story.html, (last visited March 5, 2019.)

questions the gathering and storing of individuals facial geometry.[31] The principal concerns with the existing laws requiring consent is that the individual usually has no other option than to consent. Though there is a perceived notion that individuals have the right to choose how their biometrics are used, stored, and shared, do they really have a choice?

Integrity and Trustworthiness

Biometric technology isn't just a password that can be easily changed. It is technology that identifies you by something that is part of you which is immutable. If these identifiers are copied and hacked there is almost no way to change your password unless you change your fingerprint. Issues arise with the integrity of biometric data. Biometric data once gathered must be imputed and assigned by an individual accurately. This constitutes a potential for information data to be incorrectly assigned.[32] Which creates a demand for a invincible and accurately designed data collection process. Unlike unintended disclosure of a password, unintended disclosure of biometrics creates grievous consequences that are very difficult to remediate the exposure.[33] A breach of biometric data cannot be readily corrected by simply implementing a new password. Lack of discussion and concerns of the consequences associated with errors within biometrics

[31] *Licata v. Facebook, Inc.,* 3:2015cv03748, N.D. CAL, Aug. 17, 2015, https://dockets.justia.com/docket/california/candce/3:2015cv03748/290384, (last visited March 5, 2019.).

[32] Yanick Fratantonio, et al., *Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop*, 2017 IEEE Symposium on Security and Privacy, 2017, Georgia Tech, http://iisp.gatech.edu/sites/default/files/documents/ieee_sp17_cloak_and_dagger_final.pdf, (last visited March 7, 2019.)

[33] Consensus Study Report, *Biometric Recognition: Challenges and Opportunities*, National Research Council (US), Whither Biometrics Committee, 2010, https://www.ncbi.nlm.nih.gov/books/NBK219893/, (last visited March 5, 2019.)

as well as the unintended disclosure of the data arouses much controversy. Technology errors tend to create a cloak and dagger effect. Biometric identification technology is likely to experience errors whether it be a false acceptance or false rejection. And technological parameters are set for these occurrences, but those parameters are usually set by the person who designs the technology.[34]

Health Risks

There has been an amplified desire to use biometric technology considering its intrinsic security features. One of the most coveted modalities of biometrics is the utilization of the human eye. At present there are two biometric modalities exploited for identification which are iris and retina scans. Both modalities use mathematical codes to record the data. The variance between the two is that Iris scans use subtle infrared illumination camera technology and retina scans use a low-energy infrared light beam emitted into an individual's eye.[35] Retina scans are accurate but the accuracy may be forfeited over time due to the nature of the retina tissue being affected by disease that causes degradation.[36] The preferred method is with the Iris because it is more

[34] Id.
[35] Allen Earman, *Eye Safety for Proximity Sensing Using Infrared Light-emitting Diodes*, Renesas, 2016, https://www.renesas.com/us/en/doc/application-note/an1737.pdf, (last visited March 7, 2019.)
[36] John Trader, *Iris vs. retina biometrics yes, they really are different,* SecureIDNews. 2014, https://www.secureidnews.com/news-item/iris-vs-retina-biometrics-yes-they-really-are-different/, (last visited March 7, 2019.)

reliable due to internal data components which creates stability.[37] The current ocular biometric methods use radiation which creating ionization because of the heat that is generated, which may adversely affect the accuracy and consistency. Studies show that adverse effects may occur to an eye subjected to thermal exposure. Concerns arise with the repeated exposure to infrared radiation that could cause damage to the multiple components of the eye as regenerative capabilities are very limited in most situations. One scientific model displayed a potential of laser-induced eye lesions caused by continued exposure to beams.[38] Biometric technology is frequently misunderstood, conceivably as a result of the industries lack of education and their being a deficit of regulations. This carries motive for legislation to be enacted rather than the limited guidelines that exist today. Without directed regulations and standards, public safety can and will be ignored subjecting the uninformed public to health risks.

Constitutional Protections

There is no real baseline for legal protection of biometric data because it is primarily a matter of state regulation and differs among jurisdictions. The use of biometric identifiers generates much debate

[37] M.Sujatha, K.V.S.Sravanthi, B.Jahanavi Raja, L.Dhanunjay, J.Naveen Kumar M.Sujatha, *Recognition of Human Iris Patterns for Biometric Identification*, IOSR Journal of Electronics and Communication Engineering, vol.10, pp.21-24, 2015, https://pdfs.semanticscholar.org/83d6/e6d3b8ba758abbd8f50c70540b88b9950eca.pdf, (last visited March 7, 2019.)

[38] Nikolas Kourkoumelis and Margaret Tzaphlidou, Eye Safety Relatred to Near Infrared Radiation Exposure to Biometric Devices, The ScientificWorldJournal, vol. 11, pp.520-528, 2011, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5720004/pdf/TSWJ-2011-11-902610.pdf, (last visited March 7, 2019.)

involving the challenges they create when discussing compliance with the Fourth Amendment, which includes the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[39] Here we must recognize that biometrics is implicit in the Fourth Amendment definition of persons. The courts have yet to articulate specific biometric modalities and their potential for violating the Fourth Amendment. In *United States v. Dionisio,* a case is made that heightens concerns around the expectation of privacy regarding voice prints.[40] The court's rationale was that the subpoena does not violate the Fourth Amendment thus there was no need to show probable cause. They stated that "no person can have a reasonable expectation that others will not know the sound of his/her voice."[41] Another issue with Fourth Amendment rights is that the court suggests that fingerprinting is also not intrusive therefore probable cause is not always necessary. With the expectation of privacy diminished in cases like *United States v. Dionisio,* careful attention to the consequences must be addressed, particularly as it relates to situations where automated facial recognition is litigated.

Passwords are constantly being interchanged with biometrics data which may adversely affect Fifth Amendment rights.[42] The Fifth

---

[39] Lee Epstien and Thomas Walker. *Constitutional Law for a Changing America Rights, Liberties, and Justice.* Sage Press. pp. 728-732, 2016.
[40] *United States v. Kirschner,* 823 F. Supp. 2d 665, 669, E.D. Mich., 2010, https://casetext.com/case/us-v-kirschner-2, (last visited Mrch 7, 2019.)
[41] Katz v. United States, 389 U.S. 347 , U.S. S. Ct.., 1967, https://supreme.justia.com/cases/federal/us/389/347/, (last visited March 7, 2019.)
[42] Lauren D. Adkins, Biometrics: *Weighing Convenience and National Security Against Your Privacy*, 13 Mich. Telecomm & Tech. L. Rev. 541 (2007) http://repository.law.umich.edu/mttir/vol13/iss2/10, (last visited March 7, 2019.)

Amendment protects citizens from self-incriminating testimonials and includes passwords in its definition. But in *Commonwealth v. Baust*, the Fifth Amendment did not protect against biometric passwords.[43] The court's rationale was based on the distinction between testimonial acts using mental process versus physical characteristics. The court ruled that a biometric fingerprint is not protected under the Fifth Amendment because the fingerprint is a physical characteristic.[44] There appears to be an impasse as much of legal precedent predates contemporary technology. Most devices today require both a password and a biometric identifier, therefore biometric modalities should be protected under the Fifth Amendment based upon its intended use.[45] Iphones lack the dual security of having to enter both a password and a biometric identifier, though when your biometric identifier fails, device then requires your numeric password.[46] In this scenario, we cannot confirm whether you would be protected by the constitution or not.[47]

---

[43] *Commonwealth v. Baust,* 89 Va. Cir. 267 (2014).

[44] Kyle J. O'Brien *Rethinking Fingerprints under the Fifth Amendment, American Bar Association, Aug. 9, 2017,* https://www.americanbar.org/groups/young_lawyers/publications/tyl/topics/cybersecurity/rethinking-fingerprints-under-fifth-amendment/, (last visited March 7, 2019.)

[45] Jack Linshi, *Why the Constitution Can Protect Passwords But Not Fingerprint Scans,* Time, 2014 http://time.com/3558936/fingerprint-password-fifth-amendment/, (last visited March 7, 2019.)

[46] Reed Albergotti, *Judge Rules Suspect Can Be Required to Unlock Phone With Fingerprint,* The Wall Street Journal, Oct. 31, 2014, https://blogs.wsj.com/digits/2014/10/31/judge-rules-suspect-can-be-required-to-unlock-phone-with-fingerprint/, (last visited March 7, 2019.)

[47] Jack Linshi, Why *the Constitution Can Protect Passwords But Not Fingerprint Scans*, Time, 2014, http://time.com/3558936/fingerprint-password-fifth-amendment/, (last visited March 7, 2019.)

The 229 year old law provides superior constitutional protections to a numeric password rather than your own fingerprint. We must question why there are no disclaimers provided when purchasing devices with biometric capabilities stating that when using the biometric password we relinquish our Fifth Amendment rights. We have arbitration disclaimers in most contracts that waive our right to trial by jury, therefore shouldn't there be a disclaimer for other rights that we unknowingly waive?

Legislation

With the emergence of possibilities within biometric technology industries, multiple legal issues concerning privacy eventualities must also be considered. Biometric technology is not just utilized in the public sector, it is becoming customary in the private sector. This means that biometric information data is currently being collected and stored. Concerns arise encompassing privacy and use of this data. Due to these concerns, the demand for regulation becomes imperative. Some of these issues and concerns regarding privacy rights and data protection within the realm of biometrics have been addressed and acknowledged in a many jurisdictions.[48] Illinois was the first state legislature to enact the Biometric Privacy Act, 740 ILCS 14/1 et seq. (BIPA) in 2008. It was initially introduced as Senate Bill 2400 by State Senator Terry Link and is considered the most stringent law that regulates biometrics. BIPA does not prohibit the collection of biometric data but it provides standards that private entities should follow when obtaining and storing biometrics. BIPA requires written consent along with prior disclosure of the purpose for in which the

[48] James Fullmer, Cybersecurity 2018 – The Year in Preview: Biometrics Security Privacy and the Law (2017), https://www.securityprivacyandthelaw.com/2017/12/cybersecurity-2018-the-year-in-preview-biometrics/ (last visited Jan 26, 2019).

collection of biometrics data is required. It also requires prior notification of the length of time in which this distinct biometric data will remain stored.

BIPA is now over a decade old and still remains the only biometric statute that bestows a right of private action. Texas and Washington are the only other states that have passed legislation specifically addressing biometric data.[49] What BIPA has that the other two states do not is that it permits a private right of action for violations, which means individuals may sue for violations of the statute's provisions.[50] This means that the Act provides "[a]ny person aggrieved by a violation of th[e] Act to bring suit to recover liquidated or actual damages, attorneys' fees, litigation expenses and other relief, including injunctive relief."[51]

The case *Santana v. Take-Two,* involved 3D mapping with the use of cameras to create avatars of gamers. This is one case in which the courts dismissed BIPA claims due to their lack of Article III standing.[52] The court did not accept as valid the Plaintiffs' allegations of a material risk, in part because they were unable to articulate a real injury. The

[49] 740 Ill. Comp. Stat. 14/10 (2008); 11 Tex. Bus. & Com. Code Ann. § 503.001 (West 2009); H.B. 1493, 65th Leg. Reg. Sess. (Wash. 2017)

[50] See Lara Tumeh, Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law, BLOOMBERG BNA (Oct. 16, 2017), https://www.jdsupra.com/legalnews/washington-s-new-biometric-privacy70894/

[51] Laney Gifford, Zachary Madonia & J. Thomas Richie, Illinois Supreme Court Adopts Expansive Interpretation of Standing under Illinois BIPA, Potentially Opening the Flood Gates for Class ActionsDeclassified(2019), https://www.classactiondeclassified.com/2019/02/illinois-supreme-court-adopts-expansive-interpretation-standing-illinois-bipa-potentially-opening-flood-gates-class-actions/ (last visited Feb 6, 2019).

[52] Id.

matter that has been questioned in recent years is the scope of BIPA and its Article III parameters.[53] In a recent court opinion filed on January 25, 2019 in *Rosenbach v. Six Flags Entertainment Corporation*, the Illinois Supreme Court adopted a broad interpretation of the word "aggrieved" which has expanded the right to sue under BIPA as it relates to injury.[54] Based upon this decision, it is likely other states will adopt biometric laws.

Many states realize the pressing necessity to regulate the adverse effects of biometric technology on privacy but only Illinois, Washington and Texas have enacted biometric specific privacy laws. [55] States like California, Michigan, New Hampshire, Montana, Idaho, Massachusetts, Delaware and others across the country have comparable pending laws before their legislature.[56] Many of the proposed laws aim to impose notice/consent requirements and the disclosure of how it will be stored and the eventual destruction. Other states that have strong privacy measures are attempting to include biometric modalities.[57] Biometric

[53] See also *Katz v. Donna Karan Co., L.L.C.*, 872 F.3d 114(2017); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013) on Article III standing.
[54] *Rosenbach v. Six Flags Entertainment Corp*., No. 123186 (Ill. 2018)
[55] Karla Grossenbacher & Christopher W. Kelleher, *Hazards Ahead: Uptick in Biometric Privacy Laws Can Put Employers in Hot Seat*, EMP. L. LOOKOUT (Oct. 3, 2017), https://www.laborandemploymentlawcounsel.com/2017/10/hazardsahead-uptick-in-biometric-privacy-laws-can-put-employers-in-hot-seat/
[56] See Michigan, 2017 Bill MI H.B. 5019; New Hampshire, 2017 Bill NH H.B 523;Alaska, 2017 Bill AK H.B. 72;Montana, 2017 Bill MT H.B. 518; Massachusetts, 2017 Bill MA H.B, 1985; Massachusetts, 2017 Bill MA S. 95; Delaware, Bill DE; California, Bill CA S. 327; Idaho, 2017 Bill ID S, 1033.
[57] James Fullmer, *Cybersecurity 2018 – The Year in Preview: Biometrics*, Security Privacy and the Law, 2017, https://www.securityprivacyandthelaw.com/2017/12/cybersecurity-2018-the-year-in-preview-biometrics/ (last visited Jan 26, 2019).

modalities shouldn't just be considered as an algorithm, they are part of the human individual.

Before there is full-scale use of biometric technology in society there needs to be established rules and regulations. Guidelines and standards are not enough to hold entities accountable for the safety of individual's identifying data. Most biometric data is digitally stored, therefore it allows for it to be circulated rapidly. Due to our advancements in technology it has become seemingly rudimentary to exchange data. Regulating the storage, retrieval, and use that data requires a uniform approach.[58] At this time, biometric protections generate more problems than they do solutions because of jurisdictional debates. There are currently bills in both houses of Congress. One of those is the Consumer Privacy Protection Act of 2017 which is Senate Bill (S.) 2124 and House of Representatives Bill (H.R.) 4081. Senate Bill 2124 was referred to the Senate Judiciary Committee in November of 2017 and H.R. 4081 was introduced in October of 2017. In Section 3(11)(D) of Senate Bill 2124, is a definition of "[u]nique biometric data, such as face print, fingerprint, voiceprint, a retina or iris image, or any other unique physical representation," that is to be included under sensitive personally identifiable information in an "electronic or digital form that identifies or could be used to identify a particular person."[59] The bills before Congress delineates how "misuse of sensitive personally identifiable information has the potential to cause serious or irreparable harm to an individual's livelihood."[60] Congress also found that it is

[58] Sharon Roberg-Perez, *The Future Is Now: Biometric Information and Data Privacy*, 31 Antitrust 3, 2017, https://www.robinskaplan.com/~/media/pdfs/the future is now biometric information and data privacy.pdf?la=e, (last visited March 7, 2019.).
[59] *Consumer Privacy Protection Act 2017*, https://www.congress.gov/bill/115th-congress/senate-bill/2124, (last visited March 7, 2019.)
[60] Id.

important for "business entities that own, use, store, or license sensitive personally identifiable information to adopt reasonable policies and procedures to help ensure the security and privacy of sensitive personally identifiable information".[61] Though before the houses of Congress for more than a year, the evidence of the need for regulation and the increased use of biometrics demands legislative attention, both federally and within the states.[62]

Important Trends in Biometric Data Security

According to recent reports, the biometric market was valued at USD $13.89 billion in 2017 and is forecasted to reach $41.80 billion in 2023.[63] Technology such as fingerprint, face, and iris scans have become the norm and an integral part of our society. It appears that biometric technology is in a Thomas Kuhn revolution cycle.[64] Biometics is in a model crisis on the brink of a revolution and a paradigm shift. Traditional passwords and punch cards are disappearing and new technologies are emerging. These technologies include gestural, heart rhythm, gait analysis and chemical biometrics that are derived from DNA, body odor, and even perspiration. There are already hybrid technologies being developed such as the Nokia's vibrating

[61] Id.
[62] J.C. Pierce, *Shifting Data Breach Liability: A Congressional Approach*, 57 Wm. & Mary L. Rev. 975, 985, 2016, https://scholarship.law.wm.edu/wmlr/vol57/iss3/6/, (last visited March 7, 2019.)
[63] *Biometric System Market*, Market Research Firm, https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html, (last visited March 7, 2019.)
[64] *The Kuhn Cycle*, thwink.org, http://www.thwink.org/sustain/glossary/KuhnCycle.htm, (last visited Feb. 28, 2019.)

magnetic ink tattoos (US Patent 8,766,784)[65] and a password pill from Proteus Digital Health which are in our near future.[66] Then we have the password pill from Motorola and Proteus Digital Health.[67] Regina Dugan, the current VP of Motorola, says that they are making the authentication process "more human."[68] She describes the process of taking the pill as turning you into a cyborg making your "arms like wire, hands like alligator clips" and when a device is touched you're automatically authenticated.[69] There is even technology using Spatial Phase Imaging (SPI) Sensors which extract three-dimensional (3D) information without being scanned or using structured lighting.[70] That means your biometric data can be collected anywhere anytime without your knowledge just by walking down the street in public.

As biometrics are entering mainstream use by consumers, corporations will also be increasing the integration of these systems. Airports will be increasing their use of biometric passports and biometric check-ins will

[65] *Coupling an electronic skin tattoo to a mobile communication device*, Google Patents, https://patents.google.com/patent/US20130297301A1/en, (last visited March 1, 2019.)
[66] J.R. Ehrenfeld, *Industrial Ecology: Paradigm Shift or Normal Science?,* American Behavioral Scientist, Oct. 1, 2000, https://journals.sagepub.com/doi/10.1177/0002764200044002006, (last visited March 1, 2019.)
[67] Kim Lachance Shandrow, *Swallow This 'Password' Pill to Unlock Your Digital Device*s, Entrepreneur, Feb. 3, 2014, https://www.entrepreneur.com/article/231182, (last visited March 7, 2019.)
[68] Id.
[69] Id.
[70] Photon-X – SPI Technology, Photon-X, http://www.photon-x.co/#technology, (last visited March 7, 2019.).

become customary.[71] As of January 2019, Miami passengers who are flying Lufthansa Flight 461 can now board simply by having their face scanned rather than using their boarding pass or passport.[72] According to a recent report by Société Internationale de Télécommunications Aéronautiques (SITA), 77% of airports and 71% of airlines are planning on implementing biometric technologies or investing in biometric research and development within the next few years.[73] By 2020 all smart devices, which includes phones, tablets, and wearables, will have biometric security enablement.[74] With the consumer shopping trend turning away from department stores and toward online purchases, individuals can easily pay for their items with their biometric identifiers straight from their phone. There is also a high demand for certainty in patient identifications in the healthcare industry. It is predicted that the demand for biometric identifications in healthcare

[71] Marisa Garcia, *Biometric Technology Is Taking Off As 77% Of Airports and 71% Of Airlines Review Digital ID Options*, Forbes(2018), https://www.forbes.com/sites/marisagarcia/2018/09/29/biometric-technology-is-taking-off-as-77-of-airports-and-71-of-airlines-review-digital-id-options/#4f4c8eb6704d, (last visited March 7, 2019.)

[72] *Now boarding from MIA: facial recognition departures*, Miami International Airport, Feb. 1, 2019, https://news.miami-airport.com/now-boarding-from-mia-facial-recognition-departures/, (last visited March 7, 2019.).

[73] *Air Transport Cybersecurity Insights 2018,* SITA, https://www.sita.aero/resources/type/surveys-reports/air-transport-cybersecurity-insights-2018, (last visited March 7, 2019.)

[74] Rachel German & K. Suzanne Barber, *Current Biometric Adoption and Trends*, May 2018, The University of Texas at Austin Center for Identity, https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf, (last visited March 7, 2019.)

will increase by 22.9% in 2025.[75] Biometrics will continue to innovate and be a driver in technology transformation of information security.

Conclusion

Though it may appear that biometric identifiers are annexing the security industry, passwords aren't going away. We see throughout the research that biometric technologies have their challenges and work best when supplemented with passwords. For companies that utilize biometric identifiers, whether their jurisdiction has legislation in place or not, it is apparent and essential to have written policies in place. In any transaction being proactive is superior to that of being reactive. Shaving a few dollars off of office payroll with the use of biometric systems will be ineffective if the right policies are not in place and up to industry standards. Outlining the process of collecting, storing and deleting of data assists in preventing foreseeable litigation particularly if policies are not put in place. The first biometric legislation has been around over a decade, it is really time for Congress to act upon the bills that are before them. Building consumer trust with biometric data technologies is crucial to economic development and innovation. Data privacy policies must create transparency and uniformity. We must acknowledge that biometric technologies are not perfect or absolute and therefore, we must have policies in place that accommodate these

[75] Credence Research, Healthcare Biometrics Market By Technology (Fingerprint Recognition, Iris Recognition, Palm Geometry Recognition, Vein/Vascular Recognition, Other), By Applications (Record Management And Data Security, Healthcare Staff Authentication And Workforce Management, Patient Identification And Tracking, Other), By Usage Area (Hospitals And Clinics, Pharmaceutical And Medical Device Manufacturing, Research And Academia, Other) - Growth, Future Prospects, And Competitive Analysis, 2017 – 2025, Nov. 2017, Market Research Reports, https://www.credenceresearch.com/report/healthcare-biometrics-market, (last visited March 7, 2019.)

weaknesses. There is no escaping the advancement of technology, the best we can do is prepare and anticipate the challenges.