THE FACE-ID REVOLUTION: THE BALANCE BETWEEN PRO-MARKET AND PRO-CONSUMER BIOMETRIC PRIVACY REGULATION

Kelly A. Wong*

I. Introduction

Imagine a world where a customer can pay for an ice cream cone simply by the measurement of their facial features.[1] With the recent advances in facial recognition technology, such a novel concept may soon become reality.[2] Facial feature recognition is a facet within the umbrella of biometric data, the most unique and unalterable information that one can tender to another.[3] The National Institute of Standards and Technology ("NIST") defines biometric data as the measurement of innate physiological characteristics such as fingerprints, the iris, or facial features, used for the identification of a

* J.D. Candidate, Suffolk University Law School, 2020; B.A. in Economics, College of the Holy Cross, 2017. Kelly can be reached at kellyawong1995@gmail.com.

[1] *See* Katherine Bindley, *Facial Recognition Goes Mainstream*, WALL STREET J. (Sept. 18, 2018), *archived at* https://perma.cc/3A9G-5HZS (describing a fast food restaurant's plans to change the manner in which customers pay for their products by using facial recognition technology).

[2] See Maria Korolov, *What is biometrics? 10 physical and behavioral identifiers that can be used for authentication*, CSO (Feb. 12, 2019), *archived at* https://perma.cc/VJF2-LRLN (reporting that sixty-two percent of companies are using biometric authentication and twenty-four percent of companies plan to implement it within two years).

[3] *See* Claire Gartland, *Biometrics Are a Grave Threat to Privacy*, N.Y. TIMES (July 5, 2016), *archived at* https://perma.cc/AM4A-7CVU (articulating biometric identifiers are unique and unchanging).

specific individual.[4] But the world of biometric data is not limited to solely physiological characteristics, as biometric data can also encompass behavioral characteristics, such as the measurement of human behavioral patterns.[5] As emerging technology continues to employ biometric data as a security feature, the unchangeable nature of our biometrics render these privacy features far different from a traditional, written password.[6] Because of this rapid development and the heightened sensitivity of our biometric data, it is necessary for federal regulations to evolve as well in a way that adequately protects consumer privacy.[7]

This Note addresses the need for a uniform federal regulation concerning biometric data, in light of the increased use of this technology in commonplace consumer products. The European Union's General Data Protection Regulation ("GDPR") Privacy by Design mandate in conjunction with current state biometric laws and the proposed Commercial Facial Recognition Privacy Act of 2019 could serve as a desirable blueprint for the federal regulation of biometric data. Biometric data's immutable nature heightens the consequences of misappropriation, thus increasing the likelihood for a

---

[4] *See Biometrics*, NAT'L INST. OF STANDARDS & TECH. (July 11, 2018), *archived at* https://perma.cc/52TG-8ATV (defining biometrics and it is not limited to fingerprint, iris, and facial features).

[5] *See* Nasir Memon, *How Biometric Authentication Poses New Challenges to Our Security and Privacy [In The Spotlight]*, IEEE SIGNAL PROCESSING MAG., (July 11, 2017), *archived at* https://perma.cc/5L7Y-REHD (stating biometric data encompasses physical and behavioral characteristics).

[6] *See* Paul Rubens, *Biometric Authentication: How It Works*, ESECURITY PLANET (Aug. 18, 2012), *archived at* https://perma.cc/E6P7-G4GF (stating that fingerprints, palm or finger vein patterns, iris features and voice or face patterns are common biological characteristics); *see also* April Glaser, *BIOMETRICS ARE COMING, ALONG WITH SERIOUS SECURITY CONCERNS*, WIRED (Mar. 9, 2016), *archived at* https://perma.cc/4NMG-PKE7 (asserting that biometrics are extremely sensitive personal information because of its immutability, a person cannot get their biometric back so they are left exposed). "You can't get back another ear." *See* Glaser, *supra*. *See also* Korolov, *supra* note 2 ("While it's easy to issue a new password when the old one has been compromised, you can't issue a new eyeball.").

[7] *See Biometric Data in the Workplace Could Trigger Privacy Litigation Wave*, JONES DAY (Nov. 2017), *archived at* https://perma.cc/MQ37-5DX7 (stating there is no current federal regulatory regime). *See also* Carissa Ratanaphanyarat, *Biometric Privacy Laws: Do They Exist and Why Should You Care?*, NEXTADVISOR (Sept. 6, 2018), *archived at* https://perma.cc/PHS8-8JRC (pointing to companies that incorporate biometric data in their products and services such as Apple, Facebook, and MasterCard).

consumer to be harmed by privacy breach. Where corporations are obliged to store and protect this sensitive data, measures should be taken to appropriately hold them accountable in the event they do not. Part II of this Note introduces the backdrop of biometric data identification and authorization, and discusses the current legal framework surrounding it, which exists solely as state law. Part III of this Note addresses three significant cases that are shaping the manner in which the recent laws concerning biometric privacy law are being interpreted in Illinois. Part III also addresses the Commercial Facial Recognition Privacy Act of 2019 and Privacy by Design. Finally, Part IV analyzes the current biometric regulatory framework and proposes a solution for a more effective federal regulatory system.

II. History

A. Biometric Data

You cannot see your own face, but each time you look in the mirror, your brain collects and stores biometric information to allow you to remember what you look like.[8] At the most basic level, biometric technology works in the same way by measuring the thousands of unique characteristics of an individual's face and recording the information for later use.[9] Although the use of biometrics may seem futuristic, some research suggests that the process of identifying people through physiological and behavioral characteristics dates back to nearly 31,000 years.[10] In 1858, handprints were first recorded to distinguish employees from one another.[11] Throughout the remainder of the 1800s, the scope of biometric data extended to other areas of anthropometrics, the study of the body's measurement and capabilities.[12] This subsequently led to the creation of fingerprint classification systems as humans, while each having a

[8] *See* Stephen Mayhew, *History of Biometrics*, BIOMETRICUPDATE.COM (Oct. 21, 2018), *archived at* https://perma.cc/A8XT-KVW9 (asserting human face recognition as the oldest and most basic example of biometric data).
[9] *See id.* (providing an overview of the technology).
[10] *See id.* (illustrating handprints surrounding paintings that are thought to "have acted as an unforgettable signature" in a cave estimated to be 31,000 years old).
[11] *See id.* (indicating hand and finger images were taken for identification purposes).
[12] *See id.* (extending the study of biometrics to anthropometric information).

unique fingerprint, share similar anthropometric information.[13] In 1986, a patent was granted for the notion that the iris could be used for biometric identification purposes, with a second patent awarded for the first iris recognition algorithm in 1994.[14] All of the aforementioned events have in some manner paved the way for the collection of biometric data in the consumer market through the Apple iPhone.[15]

As society continues to incorporate biometrics, it is important to recognize the difference between biometric identification and biometric authorization.[16] Biometric identifiers are used to identify "who you are".[17] Examples of biometric identifiers include, but are not limited to, fingerprints, vein patterns, iris features, and voice or face patterns.[18] Thus, biometric identification can succinctly be described as using an individual's biometric identifier to match the identifier with that specific individual within a database of biometric identifiers compiled from multiple individuals.[19] In contrast, biometric authentication is used to prove "who you are" through the

[13] *See id.* (defining anthropometrics as body measurements, physical descriptions and photographs; and further explaining fingerprint classification was created to replace anthropometrics); *see also* Glaser, *supra* note 6 (stressing that police enforcement has been fingerprinting for over 100 years and have been using biometric databases since the 1980s).

[14] *See* Mayhew, *supra* note 8 (describing that a patent was awarded to two doctors for their idea that the iris could be used for biometric identification purposes and led to the development of an algorithm to automate the process).

[15] *See id.* (recognizing that Apple utilizes Touch ID which allows consumer to unlock their device via their fingerprint and make purchases on apps through the authentication of Apple Pay). *See also* Glaser, *supra* note 6 (highlighting that Apple uses fingerprint identification in their Apple home button, MasterCard wants to use heartbeat data for the verification of purchases, and that Google's Abicus Projects plans to monitor your speech and the manner in which you walk and talk).

[16] *See* Alan Goode, *Biometric Identification or Biometric Authentication?*, VERIDIUM (July 11, 2018), *archived at* https://perma.cc/BHV9-UFBR (noting the confusion between biometric identification and authentication).

[17] *See id*. (providing that the answer to the question of biometric identification is posited as "who are you"). *See also* Rubens, *supra* note 6 (highlighting that a two-factor system can be based on measurable biological and behavioral characteristics or "something they are").

[18] *See* Rubens, *supra* note 6 (stating that fingerprints, palm or finger vein patterns, iris features, and voice or face patterns are common biological characteristics).

[19] *See* Goode, *supra* note 16 (explaining that in the situation where an organization has to identify a person, the organization uses a biometric identifier from the individual and then searches their biometric repository to identify the person). *See also* Glaser, *supra* note 6 (exemplifying that in the identification process an image is run alongside a database of images).

use of a biometric identifier.[20] For example, when the biometric system is the sole authenticator, the biometric identifier is placed against a database containing your biometric data, ensuring that your biometric identifier matches the database's stored information.[21] Today, the most commonly used types of biometric authentication technologies include retina scans, iris recognition, finger scanning, finger vein ID, facial recognition, and voice identification.[22]

B. Biometric Data in Consumer Products and Services

The use of current authentication methods such as passwords will most likely become obsolete in the near future because of the ubiquity of biometric technology.[23] Although biometrics have been around for a while, companies like Apple and Samsung are striving to implement biometric authentication into their products to prevent hackers from accessing an individual's personal information.[24]

[20] *See* Goode, *supra* note 16 (explaining that biometric data goes against database). *See also Biometrics: authentication and identification (definition, trends, use cases, laws and latest news)- 2019 review*, GEMALTO (Nov. 13, 2019), *archived at* https://perma.cc/9KMC-HB3T [hereinafter *Biometrics: authentication and identification*] (stating that authentication is comparing data from a person's identifiers to that person's biometric "template" in order to find a match).

[21] *See* Goode, *supra* note 16 (exemplifying that if a person puts their finger on a smart mobile device fingerprint sensor and the fingerprint matches what the device's data has, then the phone will unlock).

[22] *See* Margaret Rouse, *Biometric Authentication*, SEARCHSECURITY (Dec. 2014), *archived at* https://perma.cc/PUY6-XWYD (listing the types of biometric authentication processes).

[23] *See* David Gilbert, *Which Biometric Authentication Method Is Most Secure*?, SAMSUNG INSIGHTS (Mar. 1, 2018), *archived at* https://perma.cc/6W7Y-NGSZ (declaring that passwords will be replaced by biometric authentication because of its rapid adoption); *see also* Joel Snyder, *Leveraging Biometric Authentication to Improve Mobile Security*, SAMSUNG INSIGHTS (June 21, 2018), *archived at* https://perma.cc/G5MP-S2H9 (opining that passwords are bad and it's easy to switch to biometric authentication on a smart phone device); *see also What are biometrics and biometric solutions?*, SAMSUNG DEVELOPERS (Sept. 4, 2019), *archived at* https://perma.cc/KGW5-73XP (pointing to surveys demonstrating that users prefer biometric authentication and believe it is safer than passwords).

[24] *See Authentication*, APPLE (Sept. 6, 2019), *archived at* https://perma.cc/8PLT-YYWB (supporting the use of biometric authentication because of its security and convenience); *see also About Face ID advanced technology*, APPLE (Nov. 7, 2018), *archived at* https://perma.cc/PDE6-85Z7 (guaranteeing that Apple's Face ID

technology is a secure authentication method to protect the personal information embedded in an individual's Apple product). Apple states that the biometric information that it collects, mathematical representations of a user's face, is encrypted with a key only accessible by Secure Enclave. *About Face ID advanced technology*, *supra.* Apple claims that the biometric information it collects does not go into the iCloud, however, Apple does constantly update your facial recognition data into the Secure Enclave for an enhanced consumer experience when unlocking the iPhone. *Id.* The decision to un-enroll an individual's biometric data is given to the consumer through the Settings feature and it deletes all the biometric data entered. *Id. See* Malcolm Owen, *Siri could recognize user's voice patterns for identification in future iPhone or iPad*, APPLEINSIDER (Oct. 16, 2018), *archived at* https://perma.cc/HM7Z-Q5G3 (noting that Apple has filed a patent for voice authentication). *See What are the biometric authentication features on Galaxy S9, Galaxy S9+ and Galaxy Note9?*, SAMSUNG (Sept. 6, 2019), *archived at* https://perma.cc/2MDS-67GB (listing fingerprint scanning, face recognition, and iris scanning as biometric authentication methods available on their devices because of its convenience and its security); *see also Knox Platform for Enterprise: Root of Trust*, SAMSUNG KNOX (Feb. 24, 2019), *archived at* https://perma.cc/ZG4Y-5274 (implementing data encryption through Sensitive Data Protection, encrypts data on device and decrypts data when phone is turned on, in conjunction with hardware-backed Root of Trust). Hardware-backed Root of Trust secures data at the hardware level rather than the software level, making them more difficult to destabilize in the event of a hack. *See Knox Platform for Enterprise: Root of Trust*, *supra. Compare My Disney Experience – Frequently Asked Questions*, DISNEY (Feb. 24, 2019), *archived at* https://perma.cc/5LW9-YP99 (using Ticket Tag fingerprint authentication to manage individuals re-entering the park) *with Unlock with your fingerprint*, GOOGLE (Feb. 24, 2019), *archived at* https://perma.cc/C846-R6NV (conceding that fingerprint authentication can be less secure than a passcode and that a copy of an individual's fingerprint could be used to unlock an individual's device). *See also* Glaser, *supra* note 6 (recognizing that biometrics are complex in that once a biometric is compromised, an individual is essentially left without recourse because you can't obtain that biometric back); Alex Perala, *Report Predicts Rise of Face Scanning Mobile Software, and Fall of Fingerprint Sensors*, MOBILEIDWORLD (Sept. 4, 2018), *archived at* https://perma.cc/22AR-AY8H (clarifying that biometric authentication is dependent on software systems, however, Apple and Samsung use more secure systems that requires a sophisticated hardware system). *See also* FEDERAL TRADE COMMISSION, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES i (FTC Oct. 2012), *archived at* https://perma.cc/AGL3-WR4Z [hereinafter FACING FACTS] (describing the different uses for biometric data such as face identification). There are virtual makeover applications that allow you to take a picture of yourself and based on that photo, an individual's facial measurements are taken, then the hairstyle is imposed on the consumer's face. *Id. See also* Stacy Cowley, *Banks and Retailers Are Tracking How You Type, Swipe and Tap*, N.Y. TIMES (Aug. 13, 2018), *archived at* https://perma.cc/75JL-E4UH (stating that companies track how individuals move around the bank website to ascertain whether an intruder is in the account).

Nonetheless, companies are not only using biometrics for authentication and security reasons, biometrics present an unparalleled opportunity for companies to collect a consumer's distinctive data for marketing purposes.[25] Given the ever-growing presence of biometrics in the lives of individuals, there must be effective regulation that governs the security of these systems and allows consumers the freedom to control their privacy.

[25] *See* Kelly Weill, *Amazon and Walmart Want to Read Your Vital Signs (and Sell You Stuff*), THE DAILY BEAST (Oct. 11, 2018), *archived at* https://perma.cc/3HKD-AZAY (cautioning that Amazon's patent for voice recognition on the Alexa will be able to identify your moods and market products based on it). Walmart's patent is a shopping cart with biometric technology that will be able to assess your mood and send an employee to offer assistance and will also have an interactive screen that will advertise products based on your biometric information. *Id. See also* Rhett Jones, *NFL Players Strike a Deal to Sell Their Biometric Data*, GIZMODO (Apr. 24, 2017), *archived at* https://perma.cc/N4TD-SME5 (criticizing football players that signed a license agreement with Whoop to sell their biometric data for marketing strategy). *See* Kirsty Nunez, *BIOMETRICS APPLICATIONS IN MARKETING RESEARCH: GAME CHANGING MARKETING RESEARCH #2*, AMERICAN MARKETING ASSOCIATION (Apr. 13, 2015), *archived at* https://perma.cc/44G6-QQXT (explaining that certain biometric identifiers are more helpful than others in market research and discusses in turn eye tracking, facial coding, galvanic skin response, and heart rate monitoring). "Marketing researchers employ biometrics to measure physical responses to different stimuli such as online, television or print advertising, a product or service." *Id. See also* Matthew Handrahan, *Biometrics: The Science Of Play*, GAMESINDUSTRY.BIZ (Aug. 14, 2012), *archived at* https://perma.cc/8AQE-QKHE (articulating that biometric sensors in video games can collect more information on an individual's tastes and habits, which will help video game developers to create a more tailored experience for its users). In discussing the impact of biometrics on the video game industry

> Player Research now counts EA, Sony, Disney, Codemasters, Splash Damage, Natural Motion, and the BBC among its clients, and the idea that a game's designers always know best is no longer such a hard sell. The fact that figures like Gabe Newell and Sony's Shuhei Yoshida have spoken publicly about the long-term potential for Biometrics has been a great help, of course, but as the industry becomes more hit-driven a deeper understanding of what motivates players will be a powerful tool.

Id.; *see also* FACING FACTS, *supra* note 24, at 5 (illustrating that a camera on a kiosk can help advertisers ascertain the demographics of an individual when the person stands in front of it, allowing advertisers to market relevant products).

C. The Federal Trade Commission and Biometrics

Data privacy law is an emerging area of law that lacks standardized federal regulation in the collection and use of personal data.[26] However, there are some significant federal privacy laws that regulate the collection and use of data.[27] The Federal Trade Commission Act ("FTC"), the Gramm-Leach-Bliley Act ("GLBA"), and the Health Insurance Portability and Accountability Act ("HIPAA") are among the most impactful.[28] The common thread of all of these data privacy regulations is that they follow the Fair Information Practices ("FIPs") which promulgates a set of principles for information privacy through a notice and consent model.[29]

Congress enacted the FTC to protect consumers in the marketplace and to promote competition.[30] In the context of data and privacy protection, the FTC has the power to bring an enforcement action against companies who have engaged in unfair or deceptive practices such as non-compliance with privacy policies and

---

[26] *See* Leuan Jolly, *Data protection in the United States: Overview*, THOMSON REUTERS (2018) (pointing out that there is no uniform federal regulation for data collection and use).

[27] *See id.* at 2 (noting that although there isn't a comprehensive federal law regulating data privacy, there are prominent federal privacy laws that aim to regulate the collection and use of data).

[28] *See id.* at 2–3 (listing notable federal privacy laws in place).

[29] *See Fair Information Practice Principles*, CIPP GUIDE (Jan. 18, 2010), *archived at* https://perma.cc/7CZ5-HYRT (explaining that the fair information principles play a significant role in the development of data protection laws). The fair information practice principles outline that an individual must have notice of an entity's practice policies prior to collection through a privacy notice and individuals should have the ability to consent or reject certain uses of their personal information. *Id.* Consent by an individual is garnered through "opt in" which is affirmative consent such as marketing newsletter or special offers; and it is also achieved through "opt out" which is implicit consent that is assumed because the individual has not stated otherwise. *Id.* The fair information practices rely on self-regulation which at times does not adequately protect the consumer; however, many businesses believe that implementing stronger regulation would be too costly and detrimental to business growth. *Id.*; *see also Patient's Guide to HIPAA - Learning About HIPAA: What are Fair Information Practices and How Do They Relate to HIPAA*, WORLD PRIVACY FORUM (Sep. 18, 2013) [hereinafter *Patient's Guide to HIPAA*], *archived at* https://perma.cc/E3UZ-7EM5 (clarifying that HIPAA implements the Fair information practices).

[30] *See* FEDERAL TRADE COMMISSION, PRIVACY AND DATA SECURITY (FTC Dec. 2018) [hereinafter FTC REPORT] (noting that the Federal Trade Commission's goal is to ensure consumer protection and stimulate economic competition).

unauthorized disclosure of personal data.[31] Although the FTC does not regulate biometric data, it has promulgated a list of best practices when collecting and storing an individual's biometric data.[32] The FTC analyzed three hypothetical case studies to exemplify how these best practices would be implemented in the real world as an effort to educate companies in being responsible when using biometric technology.[33] Nonetheless, the FTC does not currently have the power to enforce its best practices or regulate biometric data.

---

[31] *See* FTC REPORT, *supra* note 30 (setting forth that the Federal Trade Commission can bring enforcement actions to hinder violations on consumer privacy); *see also* Leuan Jolly, *supra* note 26 (recognizing that the Federal Trade Commission has enforced compliance with privacy policies and initiated suits for unlawful disclosures of data). *See The Equifax Data Breach Settlement*, FEDERAL TRADE COMMISSION (July 2019), *archived at* https://perma.cc/2ZJU-576A (offering advice to consumers as to how to respond to the Equifax data breach); *see also* Glenn Fleishman, *Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says*, FORTUNE (Sept. 7, 2018), *archived at* https://perma.cc/7G2V-3PLW (stating that the FTC has oversight for breaches like the Equifax breach which most consider a deceptive and unfair practice).

[32] *See* FACING FACTS, *supra* note 24, at 2 (promulgating that the FTC's best practices encompass privacy by design, simplified consumer choice, and transparency). The principles outlined are defined as

> (1) Privacy by Design: Companies should build in privacy at every stage of product development. (2) Simplified Consumer Choice: For practices that are not consistent with the context of a transaction or a consumer's relationship with a business, companies should provide consumers with choices at a relevant time and context.
> (3) Transparency: Companies should make information collection and use practices transparent.

Id.

[33] *See id.* at ii (advising that in the situation where an entity is simply using facial detection to locate an individual's face, the entity should have reasonable data security protections, have a specified retention and disposal schedule, provide the consumer with information on the entity's purpose for collection and storage, and always obtain consent if the photograph is used for a different purpose). In the second case study, the FTC cautions that the entity should implement reasonable security measures to prevent hackers from obtaining access to biometric data, even though this data isn't being stored. *Id* at 13. Since the second case study involved digital signs with cameras on them, the FTC had a difficult time finding the proper way to obtain notice and consent in this scenario. *Id* at 15. In the third case study, the FTC opined that in situations where entities are collecting and storing biometric

D. State Biometric Law

While Congress has yet to enact any federal regulation concerning the protection and use of biometrics, a few states have taken initiative on the issue.[34] Illinois, Texas, and Washington are leading this needed movement.[35] The strongest of these legislations is the Illinois Biometric Privacy Act.[36]

1. Illinois BIPA

In 2008, Illinois passed the Biometric Information Privacy Act ("Illinois BIPA") which includes regulations for the collection and use of biometric data.[37] The legislative intent underpinning the Illinois BIPA is the acknowledgement of the unparalleled distinctiveness of biometrics; but more so, the imperativeness to protect the individual from misappropriation.[38] Under the Illinois BIPA, a biometric

data, the company should encrypt the stored data to prevent hackers from obtaining access. *Id* at 17.

[34] *See Biometric data and the data protection regulations (GDPR and CCPA)*, GEMALTO (Aug. 20, 2018) [hereinafter *GDPR & CCPA*], *archived at* https://perma.cc/E8W3-Q2P6 (recognizing that the United States does not have a comprehensive federal law in the regulation of biometric data use and collection); *see also* Mark Melodia et al., *Legal Risks and Rules of the Move to Biometrics*, N.Y. L. J. (Mar. 2, 2015), *archived at* https://perma.cc/GB49-XPBH (addressing the lack of federal regulation of biometric data in the United States, but acknowledging that HIPAA and the FTC can be applicable).

[35] *See GDPR & CCPA*, *supra* note 34 (indicating that Washington, Illinois, and Texas have state biometric privacy laws).

[36] *See* Adam Schwartz, *New Attack on the Illinois Biometric Privacy Act*, ELEC. FRONTIER FOUND. (Apr. 10, 2018), *archived at* https://perma.cc/XE6U-UP83 (stressing that the Illinois Biometric Information Privacy Act is the strongest biometric data privacy law in the United States).

[37] *See* Biometric Information Privacy Act § 15, 740 ILL. COMP. STAT. 14/15 (2008) [hereinafter BIPA] (outlining the requirements for the proper manner of collection, disclosure, and destruction of biometric data); BIPA § 5 (highlighting that the public welfare would be well-served through effective means of regulating the collection, use, storage, retention and destruction of biometric information); *see also BIPA*, § 14/1 (passing biometric regulation in 2008). *See also* Hanley Chew & Eric Ball, *The Impact of the Surge of Biometric Data Privacy Lawsuits Against Employers*, L. J. NEWSLETTERS (Jan. 2018), *archived at* https://perma.cc/C94D-3B7V (stating that Illinois passed the "BIPA" in 2008).

[38] *See* BIPA § 5 (positing that biometrics are unique to the individual; thus, once the information is comprised, the individual has no recourse and is at risk for identity theft). In enacting this Act, the legislature concedes that the ineffective regulation

identifier is defined to include a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.[39] On the contrary, any information used to identify an individual by means of an individual's biometric identifier is defined as biometric information.[40] The terms confidential and sensitive information, private entity, and written release are also defined in the Illinois BIPA.[41]

---

of biometric data would deter individuals from participating in biometric technology or biometric identification transactions. *Id.* The legislature has observed that biometric technologies are becoming prevalent in business transactions and being used in grocery stores, gas stations and school cafeterias. *Id.* "The full ramifications of biometric technology are not fully known." *Id.* It can be inferred that the Illinois BIPA attempts to address biometric technologies in the business context because it does not attempt to interfere with individual information covered by HIPAA and hospitals. *See* BIPA § 25. *See* Jay Schulman, *What you need to know about the Illinois Biometric Privacy Act (BIPA)*, RSM (Feb. 19, 2019), *archived at* https://perma.cc/7W8F-UCZX (explaining that BIPA was enacted in response to Pay By Touch's bankruptcy, a company that used fingerprint authentication for consumer purchases, which led them to attempt to sell their consumers' biometric data).

[39] *See* BIPA § 10 (excluding writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color from being a biometric identifier). Patient information covered under the Health Insurance Portability and Accountability Act and biological materials regulated under the Genetic Information Privacy Act are not considered biometric identifiers. *Id.* Even more, biometric identifiers do not include x-ray, or any image or film of a human used to diagnose, prognose, or treat an illness or other medical condition to examine scientific testing. *Id. See* Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information,* 66 KAN. L. REV. 637, 650 (2018) (discussing that the definition of a biometric identifier under BIPA is different than other biometric statutes); *see also* Natasha Kohne et al., *Unique Biometric Data Creates Unique Privacy Concerns*, N.Y. L. J. (2016), *archived at* https://perma.cc/9JJT-PT6D (listing that a biometric identifier is comprised of retina or iris scan, fingerprint, voiceprint, or hand scan or face geometry).

[40] *See* BIPA § 10 (proffering that biometric information can be acquired by means of capturing, converting, storing, or sharing an individual's biometric identifier). However, BIPA expressly outlines that information derived from the excluded list of biometric identifiers is not biometric information. *Id. See* Kohne et al., *supra* note 39 (stressing that biometric information does not include information derived from photographs).

[41] *See* BIPA § 10 (defining 'confidential and sensitive information' as "personal information that can be used to uniquely identify an individual or an individual's account or property"). Examples of confidential and sensitive information are genetic information testing, an account number, pass code, or social security number.

Section 15 of the Illinois BIPA outlines the proper retention, collection, disclosure, and destruction of biometric identifiers and biometric information.[42] More specifically, there is a requirement of notice and guidelines regarding the manner in which it must be given to an individual before a private entity collects an individual's biometric identifier or information.[43] With respect to the disclosure of an individual's biometric information or identifier, there are limits as to when this sensitive information can be disseminated and BIPA discourages private entities from profiting off of an individual's biometric information or identifier.[44] Moreover, an entity in possession of biometric identifiers and information must adhere to reasonable standards while being in control of this information.[45]

Id. A private entity does not include a state or local government agency, any court of Illinois, a clerk of the court, or a justice. *Id.* However, an individual, partnership, LLC, or other organized group is considered a private entity. *Id.* Informed written consent or an employee's release form is considered a written release. *Id.*

[42] *See* BIPA § 15 (possessing biometric information or identifiers in a lawful manner requires that a private entity have a written policy containing a retention schedule and guidelines for the destruction of biometric information and identifiers once the purpose of collecting the identifiers or information has been actualized or within three years of the individual's last contact with the private entity). It is required that a private entity adhere to its retention schedule and destruction guidelines. *Id.*

[43] *See id.* (collecting, capturing, purchasing, receiving via trade, or acquiring through other means a biometric identifier or information requires that the individual or its legally authorized representative is informed through writing that their sensitive information is to be collected or stored). The writing must also include the specific purpose for its collection and storage and the length of term of its collection, storage, and use. *Id.* The private entity must also obtain a written release by the individual or its legally authorized representative. *Id. See also* Chew & Ball, *supra* note 37 (explaining that organizations must give written notice before biometric data collection). Organizations must state the purpose for data collection and also the duration that the organization will use or retain the data for. *Id.*

[44] *See* BIPA § 15 (prohibiting a private entity from selling, leasing, trading, or profiting from biometric identifiers or information). BIPA states that disclosure or redisclosure is prohibited unless the individual consents, it completes a financial transaction authorized by the individual, it is required by state or federal law or municipal ordinance, or it is mandated by a warrant or subpoena issued by the court. *Id.*

[45] *See id.* (using the reasonable standard of care within the private entity's industry when storing, transmitting, and protecting from the disclosure of biometric information or identifiers). Private entities must protect biometric information or identifiers in the same manner or more protective than the manner in which the entity stores, transmits, and protects confidential and sensitive information. *Id.*

A notable aspect of the Illinois BIPA is that it provides individuals with a private right of action.[46] In the event of a violation of the Illinois BIPA, the statute sets forth the amount of damages that an aggrieved party is entitled to.[47] Not only does the statute provide individuals with the opportunity to collect liquidated or actual damages, it permits an aggrieved party to also receive attorney's fees and other forms of relief.[48] However, it should be noted that the Illinois BIPA does not intend to interfere with certain federal regulation in place or with "the admission of biometric identifiers in court, before a tribunal, agency, or board."[49]

[46] *See* BIPA § 20 (recognizing that an individual may pursue an action in a state court or as a supplemental claim in federal district court in the event that a person is aggrieved by a violation of the statute); *see also* Niya T. McCray, *Biometric Privacy: It's Time to Face the Litigation*, RAISING THE BAR, (June 2018), *archived at* https://perma.cc/SF6T-MR97 (stating the hallmark of the BIPA is its private right of action). *See* McCray, *supra* (insinuating that there has been increased litigation in Illinois due to the private right of action). Texas and Washington did not include the private right of action in their biometric information privacy statutes, so suits are left to the state attorney general. *Id. See* Caroline Bermeo Newcombe, *Implied Private Rights of Action: Definition, and Factors to Determine Whether a Private Action Will Be Implied from a Federal Statute*, 49 LOY. L.J 118, 120 (2017) (defining the right of private action).

[47] *See* BIPA § 20 (providing that a negligent private entity will be fined $1,000 in liquidated damages or actual damages, whichever is larger, and an intentional or reckless private entity will be fined liquidated damages of $5,000 or actual damages); *see also* Chew & Ball, *supra* note 37, at 2 (providing that violations of the statute entitle damaged party to statutory damages for each violation equal to the greater of $1,000 or actual damages for negligent violations and the greater of $5,000 or actual damages for intentional or reckless violations litigation in Illinois due to the private right of action).

[48] *See* BIPA § 20 (granting an aggrieved party reasonable attorney's fees which includes expert witness fees and litigation expenses and permits an injunction).

[49] *See* BIPA § 25 (clarifying that the BIPA shall not interfere with the admission or discovery of biometric identifiers or information in court; and that the BIPA does not apply to any agent of a State agency or local governmental unit). BIPA prohibits its application with the X-Ray Retention Act, HIPAA, Accountability Act of 1996, and any financial institution subject to Title V of the Gramm-Leach-Bliley Act of 1999. *Id.*

2. Washington Biometric Legislation

The Washington legislation which protects biometric identifiers is the 2017 Legislative House Bill 1493 ("H.B. 1493").[50] The H.B. 1493 defines a biometric identifier as "automatic measurements of an individual's biological characteristics" in the form of data.[51] The acknowledgement that Washington consumers are increasingly asked to divulge their biometric identifiers in commerce underlies the legislative intent behind the enactment of the H.B. 1493.[52] More specifically, H.B. 1493 requires that an individual is given reasonable notice prior to collecting an individual's biometric identifier and that the person obtain consent from the individual.[53] Washington legislation is more lenient in that it differentiates and provides different security standards depending on whether a biometric identifier is captured or enrolled.[54] While it may be true that a person that has obtained consent to 'enroll' an individual's biometric identifier may use it for a commercial purpose, there are situations in which a person may disclose the biometric identifiers to a third-party

[50] *See* H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017) (outlining the procedures to protect biometric data).

[51] *See id.* (providing that fingerprints, voiceprints, eye retinas, irises, or other biological patterns or characteristics used to categorize an individual are examples of biometric identifiers). H.B. 1493 excludes "physical or digital photograph[s], video or audio recording[s] or data generated therefrom, or information collected, used, or stored for health care treatment, payment or operations under the federal health insurance portability and accountability act of 1996." *Id.*

[52] *See id.* (contending that the legislature is unsettled with the collection of citizen's biometric information without notice or consent). To resolve the inconsistencies surrounding proper notice and consent, the legislature is mandating businesses to impart how it intends to use biometric data and to "provide notice to and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database." *Id.*

[53] *See id.* (contrasting notice from affirmative consent). The bill articulates that the manner in which notice is given to an individual should be reasonable given the context. *See* Wash. H.B. 1493. A person in the H.B. 1493 is defined as an individual, partnership, corporation, limited liability company, organization, association, legal or commercial entity. *Id.*

[54] *See id.* (prohibiting the use of an individual's biometric identifier for sale, lease, or disclosure for a commercial purpose unless consent has been received from an individual). H.B. 1493 defines 'enroll' as a "means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual." *Id.* The bill also states that "capture" means the process of collecting a biometric identifier from an individual. *Id.*

without obtaining consent.[55] If a person is in possession of an individual's biometric identifier for a commercial purpose, the person is required to use reasonable care to secure it and retain it for a reasonable amount of time.[56] On the other hand, a person is not obligated to provide notice nor obtain consent for biometric identifiers that are merely captured, collected, or enrolled in furtherance of a security purpose, or in the alternative, are merely captured for a commercial purpose.[57] H.B. 1493 does not provide a private right of

[55] *See id.* (stating that a commercial purpose is a "purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier."). Consent for disclosure is not necessary when disclosure is necessary to provide a subscribed to product or service, to facilitate a financial transaction requested and authorized by the individual; or authorized by federal or state statute or a court order, needed to prepare for litigation, or disclosure is made to a third-party who contractually agrees that the biometric identifier will not be further disclosed or enrolled for a commercial purpose. *Id.* If a third-party contractually agrees to non-disclosure of a biometric identifier, that third-party is still required to follow the notice and consent rules if the third-party intends to use the it for a commercial purpose. *Id*. Additionally, a person who enrolls an individual's biometric identifier for a commercial purpose or obtains an individual's biometric identifier from a third-party for a commercial purpose may not disclose it if it is contrary to the initial purpose for which it was provided, unless the person obtains the individual's consent for the new terms of use or disclosure. *Id.*

[56] *See id*. (indicating that a person in possession of biometric identifiers must exercise reasonable care to prevent unauthorized access and procurement, while also withholding the biometric identifiers for no longer than is reasonably necessary). Persons can withhold biometric identifiers no longer than reasonably necessary to (1) provide services for its enrollment purpose, (2) to safeguard against and prevent fraud, criminal activity, claims, security threats, or liability, and (3) to comply with statute, a court order, or a federal, state, or locally specified public retention schedule. *Id*. Unenrolled biometric identifiers are exempt from the disclosure and retention limitations. *Id.*

[57] *See id.* (articulating that the furtherance of a security purpose limits the restrictiveness of the statute with regards to notice and consent). Capture is defined as "the process of collecting a biometric identifier from an individual." *Id. See also* Divya Taneja, *Washington Enacts a Biometric Privacy Statute in a Departure from the Existing Standard*, PROSKAUER NEW MEDIA AND TECH. L. BLOG (June 13, 2017), *archived at* https://perma.cc/6F2X-27CA (analyzing that an entity's mere capture for a commercial purpose, rather than enrollment, relieves an entity from the statute's requirements). Unenrolled biometric identifiers which are not stored in a digital template and are a one-time use, are not subject to disclosure and retention rules. *Id.*

action like the Illinois BIPA, thus enforcement suits can only be brought forward by the attorney general pursuant to Washington's consumer protection act.[58] Additionally, H.B. 1493 does not apply to certain federal legislation and permits law enforcement to act within their scope of authority.[59] In sum, H.B. 1493 is the more business-friendly biometric legislation as compared to BIPA because of its more lenient regulations regarding the collection and use of biometric information.[60]

3. Texas Biometric Information Legislation

Texas's version of biometric legislation brings its own benefits and pitfalls.[61] In 2009, Texas enacted the Business and Commercial Code Section 503.001 ("B.C. 503.001") to protect a person's biometric identifiers.[62] The B.C. 503.001 defines a biometric identifier comparably to the Illinois BIPA; however, it does not address or define biometric information.[63] In contrast to H.B. 1493, B.C. 503.001 places

[58] *See Sensitive to the Touch: The Evolution of U.S. Biometric Privacy Law*, BRADLEY (May 2018), *archived at* https://perma.cc/Y9QU-WYAQ [hereinafter *Sensitive to the Touch*] (explaining that BIPA is the only state that has permitted "its courts to enforce biometric laws for consumer-claimants"); Wash. H.B. 1493 (providing the attorney general the sole authority to enforce H.B. 1493 under the consumer protection act, chapter 19.86 RCW). Chapter 19.86 RCW of the consumer protection act seeks to preserve business and prevent unfair or deceptive acts in trade or commerce. *Id.* The legislature asserts that H.B. 1493 was included in the consumer protection act because they believe that biometric privacy protection is essential to the public interest. *Id.*

[59] *See id*. (barring the application of H.B. 1493 to the Gramm-Leach-Bliley Act of 1999 and Title V of the Health Insurance Privacy and Portability Act of 1996). The Act does not expand or limit the state law enforcement's authority to carry out lawful search and seizure. *Id.*

[60] *See* Taneja, *supra* note 57 (drawing a distinction between the enrollment of biometric identifiers and the mere capture and stressing that the latter is not subject to the stringent requirements of the former).

[61] Kohne et al., *supra* note 39 (failing to include a definition for biometric information leading to more confusion for business but having the fastest destruction cycle out of all of the state statutes)

[62] *See* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017) (introducing legislation for biometric data privacy protection). *See* Kohne et al., *supra* note 39 (analyzing that the Texas statute does not explicitly include protection of biometric information, but only biometric identifiers).

[63] *Compare* BUS. & COM. § 503.001 (defining biometric identifier as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry without listing any specific exclusions to such identifiers, and limiting the wording of the statute to

parameters on the capture of a biometric identifier for a commercial purpose.[64] With respect to the sale, lease or disclosure of an individual's biometric identifier, a person cannot do so to another person for a commercial purpose unless

> (A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;
> (B) the disclosure completes a financial transaction that the individual requested or authorized;
> (C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or
> (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.[65]

B.C. 503.001 allows persons to store biometric identifiers but requires persons to exercise reasonable care with the biometric identifiers and implement proper destruction cycles.[66] Civil penalties

---

suggest the list is conclusive), *with* BIPA § 10 (providing that a biometric identifier is a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry). BIPA includes the definition of biometric information to mean the capture, storing, or sharing of a biometric identifier. BIPA § 10. *See also* Kohne et al., *supra* note 39 (questioning whether a record of hand or face geometry obtained from a photograph is considered a biometric identifier).

[64] *See* BUS. & COM. § 503.001 (requiring a person to inform an individual prior to capture of biometric identifier and to obtain consent for the capture of a biometric identifier).

[65] *See id*. (outlining situations in which a person may sell, lease, or disclose a biometric identifier to a third-party).

[66] *See id*. (proffering that persons must use reasonable care in a manner that is the same or more protective than the method in which that person stores, transmits, and protects any other confidential information in possession). Following the first anniversary of the expiration of the purpose for the collection of a biometric identifier, a person must destroy the biometric identifiers. *Id.* However, if the law requires that a biometric identifier be kept for longer than the period in subsection (c)(3), then it must be destroyed no later than the first anniversary that the identifier is no longer needed by law. *Id.* With respect to the employer–employee relationship, the purpose for the collection of a biometric identifier expires when the relationship terminates. *Id. See also* John G. Browning, *The Battle Over Biometrics: A look at the law in Texas and two other states*, TEX. B. J. (Oct. 2018), *archived at*

will be imposed upon violation of the B.C.503.001; however, the attorney general is the only person authorized to enforce an action, not an individual even if he or she is affected pursuant to the statute.[67] Texas's biometric statute is strong, however it does not meet to the standard of BIPA.

III. Premise

This Note will address three critical cases that have arisen under BIPA, which have shaped the manner in which it is interpreted. Next, this note will discuss the theory of privacy by design and how it relates to biometric privacy. Lastly, the Senate's recent introduction of the Commercial Facial Privacy Act of 2019, purposed to be the first federal regulation of facial biometric technology, presents new considerations on this subject.

A. Rosenbach v. Six Flags Entertainment Corporation

In 2016, a notable case arose under the Illinois BIPA regarding the collection of a child's biometric identifiers at Six Flags, a nationwide commercial theme park.[68] The issue was whether Six Flags properly collected a child's fingerprint information for passes to the park when Six Flags acquired it without obtaining consent or explaining what they planned to do with his biometric identifier.[69] The court focused on whether the "aggrieved party," in this case the young boy, actually accrued an injury or an adverse effect rather than a technical violation.[70] In determining whether the plaintiff was actually

https://perma.cc/3756-5G4G (recognizing that Texas has a more accelerated destruction rate than the Illinois BIPA).

[67] *See* BUS. & COM. § 503.001 (imposing a ceiling of $25,000 per violation). An attorney general is the only party permitted to enforce an action. *Id.*; Browning, *supra* note 66 (noting the attorney general has the power to enforce an action).

[68] *See* Rosenbach v. Six Flags Entm't Corp. (*Rosenbach I*), No. 2-17-0317, 2017 WL 6523910, at *1 (Ill. App. Ct. Dec. 21, 2017) (stating that this case involves the unlawful collection and possession of biometric information).

[69] *See id*. at *1–2 (summarizing that plaintiff's claim arose from the lack of consent and lack of disclosure on defendant's plan for collection, storage, use or destruction of plaintiff's biometric identifier).

[70] *See id*. at *4 (stressing that if an aggrieved party stated a technical violation as constituting being aggrieved then the word aggrieved would be superfluous). In determining the definition of aggrieved under the statute, the court looked into the plain meaning of the word and considered case law that also attempted to define the

aggrieved, the court on appeal held that the plaintiff had to allege an actual injury or harm under BIPA and not just a mere technical violation of the statute.[71] The court noted that a technical violation is not sufficient to meet the aggrieved by standard outlined in BIPA and thus a plaintiff is not entitled to recover any damages absent a showing of actual injury.[72] The holding in this case has curtailed an individual's rights to bring a claim for a violation of privacy rights because to be considered an "aggrieved party" the individual must also show an actual harm that derived from the technical violation of the statute.

In early 2019, the Illinois Supreme Court on appeal rejected the appellate court's interpretation of the "aggrieved" by standard.[73] In reversing the appellate court, the Illinois Supreme Court analyzed the "aggrieved" by standard through interpretation of its plain and ordinary meaning in conjunction with the legislature's intent in

word. *Id.* Moreover, the court posited that the legislature's intent in using the word aggrieved was intended to prevent individuals from stating claims based on a mere statutory violation. *Id. See also* Kelly Singleton, *Illinois Appellate Court Holds That BIPA Plaintiffs Must Show Actual Harm*, JDSUPRA (Mar. 28, 2018), *archived at* https://perma.cc/A9WE-5AD9 (pointing to the appellate court's decision that a person without any injury or adverse effect are not aggrieved, thus not guaranteed any damages under BIPA). *See* Rhett Jones, *Six Flags Biometric Case Could Turn One of the Toughest Privacy Laws in the U.S. Upside Down*, GIZMODO (Nov. 26, 2018), *archived at* https://perma.cc/C6QC-B7F9 (asserting that Justice Anne Burke told Six Flags' attorneys that their argument does not consider the initial violation of the statute). "How does one challenge that, if that isn't harm." *Id.* The court considers the fact that there is no opportunity for the guardian to say no or be given the information of what they could do. *Id.*

[71] *See Rosenbach I*, 2017 WL 6523910, at *4 (highlighting that a plaintiff who only states a technical violation under BIPA is not an aggrieved person); *see also* McCray, *supra* note 46 (recognizing that a plaintiff must allege more than a technical violation under BIPA).

[72] *See Rosenbach I*, 2017 WL 6523910, at *5 (holding that the plaintiff was not an aggrieved person under BIPA and cannot recover); *see also* McCray, *supra* note 46 (proffering that failure to provide notice or obtain consent is not enough to obtain damages under BIPA); *see also* Michael J. Bologna, *Six Flags' Scan of Boy's Thumbprint Tests Biometric Privacy Law*, BLOOMBERG LAW (Oct. 16, 2018), *archived at* https://perma.cc/Z32E-TK7G (analyzing that there will be a reduction in cases brought under BIPA if the court decides that a technical violation does not result in an aggrieved person).

[73] *See* Rosenbach v. Six Flags Entm't Corp. (*Rosenbach II*), 129 N.E.3d 1197, 1204, 1207 (Ill. 2019) (dismissing defendant's contention that an individual must suffer an actual harm to be an "aggrieved" person entitled to protection under BIPA).

enacting the statute.[74] The holding of the Illinois Supreme Court in sum is that an individual "need not allege some actual injury or adverse effect, beyond violation of his or her rights under the act, in order to qualify as an aggrieved person and be entitled to seek liquidated damages and injunctive relief pursuant to the act."[75] In other words, the holding of the Illinois Supreme Court has essentially turned BIPA into a strict liability statute making it easier for plaintiffs to receive damages if companies fail to comply with the provisions of the statute.

[74] *See Rosenbach II*, 129 N.E.3d at 1204 (proffering that in determining the language in contention, the court aimed to ascertain the legislature's intent in constructing the statute). The court stated that "aggrieved by" does not necessarily mean that an individual has to suffer from economic harm, rather the accepted definition is that an individual has had an invasion of a legal right. *Id.* at 1205. A violation of an individual's statutory rights occurs when an entity fails to comply with the requirements of BIPA, which include properly collecting, retaining, disclosing, and destroying biometric identifiers or information. *Id.* at 1203.

[75] *See id.* at 1206 (finding that the violation in itself is an injury to an individual and deserving of a cause of action). The use of biometric technology is so pervasive and more so puts at risk the security of an individual's biometric identifiers when the statute is disregarded. *Id.* The court substantiates its position that a failure to adhere to statute harms an individual by quoting from *Patel v. Facebook*, "the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized." *Id.* (quoting 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018)). *See also* Emily Chan, *In Federal Court, Article III Standing Remains a Defense to Illinois Biometric Privacy Claims*, PROSKAUER ROSE LLP (Jan. 30, 2019), *archived at* https://perma.cc/N2FF-2CXC (observing that the *Rosenbach* decision will lead plaintiffs to file claims in state court rather than federal court). Federal court does not give plaintiffs Article III standing for a mere violation of statute, while the Illinois courts will give plaintiffs standing for a technical violation. *See* Chan, *supra*. In an amicus brief, groups fighting for privacy rights argued that the absence of enforcement powers for the attorney general coupled with mandated statutory damages indicates that Illinois's legislature had an intent to create a robust enforcement regime that relies on private litigants to ensure compliance with BIPA's requirements of notice and informed consent. *See* Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of Petitioner/Plaintiff Urging Reversal at 17–18, Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197 (Ill. 2019) (No. 123186) [hereinafter Brief in Support of Petitioner]. *See also Rosenbach v. Six Flags–Whether an individual whose biometric data has been unlawfully collected in violation of the Illinois Biometric Information Privacy Act has a cause of action,* ELECTRONIC PRIVACY INFO. CTR. (Oct. 2, 2019), *archived at* https://perma.cc/LU9S-7RAC. The groups argued that if the court accepted Six Flags' reading of BIPA, then it would gut the statute's primary purpose and leave Illinoisans without meaningful recourse in a world of increasing technology and proliferating uses of biometric data. *See* Brief in Support of Petitioner, *supra.* This case also brings up the question as to whether a violation of someone's expectation of privacy is a harm in of itself. *Id*.

B. Rivera v. Google Inc.

In 2016, Google came under fire for one of its photo-tagging platforms and was sued under the Illinois BIPA.[76] The facts surrounding this case involve plaintiff, a Chicago resident, that claimed that Google Photos scanned her facial geometry or features from a photo and created a face template from the photograph.[77] The Plaintiff alleged that Google violated the Illinois BIPA when the corporation scanned her facial geometry without first obtaining her consent.[78] The District Court for the Northern District of Illinois had to analyze whether biometric information acquired from photographs was considered a biometric identifier under BIPA.[79] The court held that the face templates derived from photographs did constitute a biometric identifier under BIPA since Google is in essence using

[76] *See* Rivera v. Google Inc. (*Rivera I*), 238 F. Supp. 3d 1088, 1091 (N.D. Ill. 2017) (describing that the Google Photos service automatically uploads your device's photographs to its application and then the service scans the photograph and creates a template based on the face's facial measurements); *see* Jeffrey Neuberger, *Google Is the Latest Online Provider to Face Class Action over Collection of Faceprints*, PROSKAUER NEW MEDIA AND TECH. LAW BLOG (Mar. 17, 2016), *archived* at https://perma.cc/CCK6-NKNJ (expressing that Google was sued under the Illinois BIPA for its photo tagging system). *See also Search by people, things, & places in your photos*, GOOGLE (Feb. 23, 2019), *archived at* https://perma.cc/V9NC-BU5U (explaining that photo tagging is done by using the Google Photos app, tapping the search bar, a row of faces appear, and then the individual clicks a face to see more photos of the face).

[77] *See Rivera I*, 238 F. Supp. 3d at 1090 (outlining that an Illinois resident alleged that Google scanned her facial features to create a face template). The plaintiff alleges that at the time the photos were scanned, the device had an Illinois-based Internet Protocol address. *Id.* at 1091. There is ambiguity as to whether BIPA applies if the scans took place outside of the state even though the photographs were uploaded in Illinois. *Id.* at 1102.

[78] *See id.* at 1090 (providing that Google violated the Illinois BIPA by failing to obtain consent for the creation of the face template). Plaintiff alleges that the photo-tagging service can ascertain the individual's age, gender and location and that this collection without obtaining consent is a violation of BIPA. *Id.* at 1091. Plaintiffs further argue that Google did not create a retention and destruction schedule of their biometric information, which is required under BIPA. *Id.* at 1092. The court rejected Google's argument that consent needs to be obtained in person to support its argument that the photographs cannot be biometric identifiers. *Id.* at 1095.

[79] *See id.* at 1092 (discussing whether biometric information acquired from photographs are covered by the BIPA).

biology-based measurements to create a scan of facial geometry.[80] Google's argument that only face scans done in person only qualify as biometric identifiers was rejected by the Court.[81] The holding in *Rivera v. Google* has expanded what can be considered a biometric identifier under the Illinois BIPA. However, In December 2018, Google was granted summary judgement and the suit was dismissed because the court found that the plaintiffs cited a lack of concrete injuries by the collection and storage of their biometric identifiers.[82]

[80] *See id.* at 1095 (explaining that the manipulation of a biometric identifier into a piece of information such as a face scan is covered by BIPA if that information can be used for identification of an individual). *See* BIPA § 10 (excluding photographs from being considered a biometric identifier). BIPA explicitly prohibits photographs from being considered a biometric identifier, however, the court in *Rivera v. Google* is liberally construing the statute to include biological measurements from photographs to be a biometric identifier. *See Rivera I*, 238 F. Supp. 3d at 1095. The Court finds support for its argument through analyzing the definition of biometric information which states that it is any information regardless of how it is obtained. *See id.* at 1095. The legislative intent behind BIPA, the advancement of technology and concerns to privacy from it, would be diminished if the court were to limit the manner in which biometric identifiers could be obtained. *Id.* at 1095–96. A biometric identifier should not be determined by the medium in which it is obtained, but rather, should be characterized as anything that contains a "set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person." *Id.* at 1096.

[81] *See Rivera I*, 238 F. Supp. 3d at 1095 (rejecting Google's argument that face templates don't constitute a biometric identifier). Google's motion to dismiss was quashed and the case was sent to a discovery schedule. *Id.* at 1104. Google scans the photographs and turns the faces within into face templates, which the court categorizes as a "scan of face geometry," which is a biometric identifier under BIPA. *Id.* at 1095. Google argues that face scans done in person, not from a photograph, are a biometric identifier but the court proffers that it does not matter how the identifier is obtained to be considered a biometric identifier. *Id.* In rejecting Google's argument, the photograph exclusion and the other exclusions as a defense becomes toothless. *Id.* at 1097 (noting that if Google had simply stored the photos and not made a facial scan of geometry, then there would not be a violation).

[82] *See* Rivera v. Google Inc. (*Rivera II*), 366 F. Supp. 3d 998, 1006 (N.D. Ill. 2018) (deciding that because there was not a substantial risk of breach and subsequent disclosure of plaintiff's data, plaintiff can't allege a concrete harm for Article III standing). Plaintiffs' statement that they "feel aggrieved" is not sufficient to establish a concrete injury for Article III standing. *Id.* at 1005–06. People expose their faces to the public every day; so that biometric identifier is more public that a social security number, the court alleged. *Id.* at 1010. *See also* Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) (proffering that private plaintiffs must allege a concrete harm rather than one this is abstract, but the harm does not necessarily have to be tangible); *US judge dismisses suit against Google over facial recognition software*, CNBC (Dec. 29, 2018), *archived at* https://perma.cc/KRN5-N5WU

Accordingly, the court also stated that there was a lack of subject matter jurisdiction because the retention of an individual's private information is not a concrete injury to satisfy Article III.[83]

C. In re Facebook

Facebook has also garnered significant attention for its alleged violation under the Illinois BIPA through its "Tag Suggestions" platform.[84] The plaintiffs in this case are alleging that the "Tag

(explaining that the lawsuit filed against Google by consumers who claimed that Google's photo sharing and storage service violated their privacy was dismissed).

[83] *See Rivera II*, 366 F. Supp. 3d at 1005 (finding that in *Spokeo Inc. v. Robbins*, the court held that a violation of a statute is not sufficient to achieve Article III's concrete injury standard). To establish Article III standing, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.* at 1003. *See also* Eric Goldman, *Google Photos Defeats Privacy Lawsuit Over Face Scans–Rivera v. Google*, TECH. & MARKETING. L. BLOG (Dec. 31, 2018), *archived at* https://perma.cc/PC3Q-F6PC (holding that there isn't a substantial risk of identity theft using Google's face templates even though people can't change their faces). The court held that immutability does not justify an across-the-board conclusion that all vases involving any private entity that collects or retains individuals' biometric data present a sufficient risk of disclosure that concrete injury has been satisfied in every case. *Id. See also* Max Kennerly, *Rethinking Article III Standing Requirements*, LITIG. & TRIAL (Feb. 8, 2017), *archived at* https://perma.cc/9AAV-7TRJ **(**explaining that to have Article III standing, plaintiff must show that it has suffered an injury in fact, the injury is fairly traceable to the challenged action of the defendant, and it is likely that the injury will be redressed by a favorable decision); *see also* Torsten Kracht et al., *INSIGHT: Illinois Biometric Privacy Law Doesn't Require Actual Injury—What's Next*, BLOOMBERG L. (Feb. 27, 2019), *archived at* https://perma.cc/Y62U-85TX (discussing that the Supreme Court does not consider the improper collection of biometric as a concrete harm, thus hindering plaintiffs from asserting relief in federal courts).

[84] *See In re* Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535, 540 (N.D. Cal. 2018) (introducing that plaintiffs are challenging Facebook's "Tag suggestions" platform). "Tag Suggestions" is defined as an application "which scans for and identifies people in uploaded photographs to promote user tagging." *Id.* at 540–41. There is a four-step facial recognition process in which

> [T]he software tries to detect faces (the "detection" step) and standardizes any detected faces for qualities like orientation and size (the "alignment step"). For each face that is detected and aligned, Facebook computes a "face signature," which is a "string of numbers that represents a particular image of a face" (the

Suggestions" platform is a violation of BIPA since it scans and identifies individuals from their photographs and turns it into a face template without giving the individual prior notice or obtaining their consent.[85] Claiming that plaintiffs did not meet the standard and cannot obtain relief under BIPA, Facebook focused its argument on the "aggrieved party" standard articulated in the 2017 *Rosenbach* holding.[86] However, the court rejected Facebook's interpretation and held that the correct interpretation under Illinois law is that a person is aggrieved when a legal right is invaded.[87] Thus, the holding in *In re Facebook* has expanded the privacy rights for individuals which were once curtailed under the 2017 *Rosenbach v. Six Flags*[88] decision, and could lead to an influx of litigation in the foreseeable feature since the standard for being aggrieved is low.[89]

> "representation" step). Face signatures are then run through a stored database of user "face templates" to look for matches (the "classification" step).

Id. at 541.

[85] *See In re Facebook*, 326 F.R.D. at 541 (alleging that the scanning of photographs which stores facial biometric identifiers without consent or notice is a violation of BIPA).

[86] *See id*. at 545 (relying on the 2017 *Rosenbach* interpretation of an aggrieved person which is that there needs to be an actual harm beyond the statutory violation to be considered an "aggrieved" person under BIPA). The correct interpretation of the *Rosenbach* holding would be that an injury to a privacy right is sufficient to be considered an "aggrieved" person under BIPA. *Id.*

[87] *See id*. (asserting that the invasion of a legal privacy right means that a person is aggrieved); *see also* Joel Rosenblatt, *Facebook Can't Avoid Privacy Suit Over Biometric Face Prints*, BLOOMBERG (Feb. 26, 2018), *archived at* https://perma.cc/C745-GZMU (explaining that the alleged violation of the user-consent requirement in Illinois law goes to the very privacy rights the legislature sought to protect).

[88] Rosenbach v. Six Flags Entm't Corp. (*Rosenbach I*), No. 2-17-0317, 2017 WL 6523910, at *1 (Ill. App. Ct. Dec. 21, 2017).

[89] See *Oil & Gas M&A Portal – Deal Certainty*, LATHAM & WATKINS LLP (Feb. 2016), *archived at* https://perma.cc/5S8E-KA9W (stating that deal protections are in place to incentivize a buyer to close). Thus, analogous to M&A transactions, if there is a larger incentive that a plaintiff will be able to obtain damages due to a company's non-compliance, a company should be more cognizant of following the provisions of the biometric statute. *Id.*

D. Privacy by Design

The concept of Privacy by Design ("PbD") was conceived by Ann Cavoukian as an effort to bolster data privacy.[90] With the rise of an information-centric market, Cavoukian acknowledged the importance of giving consumers the freedom of choice and personal control over their personal information, including biometrics.[91] Cavoukian argues that privacy must be integrated into data systems and technologies while being approached with a design thinking perspective.[92] As a solution to the issues surrounding data privacy, Cavoukian came up with a list of seven principles.[93]

The list of seven principles that Cavoukian created seeks to provide a universal framework that companies can follow to ensure privacy protection.[94] The first on the list is that technology should be designed to be proactive not reactive; preventative not remedial.[95] Following the first, Cavoukian states two principles that privacy

---

[90] *See* Ann Cavoukian, *The 7 Foundational Principles*, PRIVACY BY DESIGN (Aug. 2009), *archived at* https://perma.cc/8QJF-7FKX (proffering that reliance on regulatory systems is not enough and that privacy assurance must be embedded in an organization's technology and data systems).

[91] *See id.* (articulating that the notion of privacy is not only a legal compliance requirement, but also a market imperative and an enabler of trusts and freedoms). Due to the rise of the knowledge creation and service delivery market, the significance of information has grown, thus increasing the need for responsible management of it. *Id.*

[92] *See id.* (describing design-thinking as a manner in which to perceive the world and overcome constraints in a holistic, interdisciplinary, innovative, and inspiring way). Cavoukian argues that we should approach privacy from a design-thinking perspective and that it must essential to organizational priorities, project objectives, design processes, and planning operations. *Id*. Privacy should embed any standard, protocol, or process that infiltrates a consumer's life. *Id.*

[93] *See id.* (listing the seven principles as (1) proactive not reactive; preventative not remedial, (2) privacy as the default, (3) privacy embedded into design, (4) full functionality, (5) end-to-end security, (6) visibility and transparency, and (7) respect for user privacy).

[94] *See id.* (stating that PbDs should be a universal framework in today's modern era).

[95] *See id.* (explaining that PbD is proactive rather than reactive since it foresees and prevents privacy incidents before they occur). The aim of PbD is to prevent privacy infractions from occurring. *Id*. In order to prevent privacy hacks, there must be methods to ascertain poor privacy designs and practices and outcomes, and to correct any negative impacts. *Id*.

should be the default and embedded into design.[96] Once embedded into design, privacy should be fully functional and have end-to-end security.[97] Lastly, to ensure user trust in technology, there must be visibility and transparency as well as respect for user privacy.[98]

In light of mounting concern for data security due to recent breaches, the concept of implementing privacy by design has been in circulation.[99] Notably, the European Union ("EU") has recently implemented PbD into their new legislation the GDPR.[100] The EU's implementation of PbD into its legislation is an acknowledgement that

---

[96] *See id.* (noting that privacy should be built into technology, thus the burden remains on the entity to protect this information, not the consumer). Privacy protection should be a default rule. *Id.* Privacy should be informed through purpose specification; collection limitation; data minimization; and a use, retention and disclosure limitation. *Id.* Privacy should be embedded into technologies in a holistic, integrative and creative manner. *Id.* Once privacy is embedded into the design of IT systems and business practices, privacy becomes an essential element of the core functionality that is being serviced. *Id.*

[97] *See id.* (clarifying that privacy should not be considered as a tradeoff but should help serve and satisfy all legitimate objectives). PbD should extend throughout the entire lifecycle of data involved and strong security measures should be implemented from start to finish. *Id*. Once data is collected, it should be securely retained and then securely destroyed at the end of the process. *Id*.

[98] *See id*. (advocating for accountability, openness, and compliance to ensure visibility and transparency). In order to establish accountability and trust, visibility and transparency are necessary. *Id*. To ensure respect for user privacy, the interests of the individual must be strongly considered through strong privacy defaults, appropriate notice, and user-friendly options. *Id*.

[99] *See* Heidi Maher, *Privacy By Design Is Important For Every Area Of Your Business*, FORBES (Apr. 10, 2018), *archived at* https://perma.cc/6H8W-QYDZ (analyzing that due to consumer's weak passwords and companies' unpatched software, the solution should be to embed privacy in the fabric of the entity). Due to data hacks that encompass identity theft and fraud, privacy by design is now being considered as a strategy for entities. *Id. See also* Frederick Leentfaar, *Privacy by design and default*, GLOBAL DATA HUB (Nov. 2016), *archived at* https://perma.cc/2EZ5-XKJV (stating that in recent years there has been adoption of PbD by regulators).

[100] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 48 (adopting Article 25 into the GDPR which requires that the controller implement only personal data that is necessary for its specific purpose). Article 25 states that the measures shall ensure by default that persona; data is not accessed without the individual's intervention to an indefinite number of individuals. *Id. See* Nate Lord, *What is GDPR (General Data Protection Regulation)? Understanding and Complying with GDPR Data Protection Requirements*, DIGITAL GUARDIAN (2018), *archived at* https://perma.cc/ABZ5-58G4 (announcing that the GDPR came into effect on May 2018 and promulgates how companies should regulate personal data).

privacy protection must be ensured through stronger methods.[101] As of right now, PbD has not been implemented into any United States legislation; however, it has been listed on the FTC's suggestions for best methods when using biometric information.[102]

E. The Commercial Facial Recognition Privacy Act of 2019

On March 14, 2019, U.S. Senators Roy Blunt from Missouri and Brian Schatz from Hawaii introduced the Commercial Facial Recognition Privacy Act of 2019 ("CFRP Act"), which aims to federally regulate consumer uses of facial recognition technology.[103]

---

[101] *See* Leentfaar, *supra* note 99 (asserting that privacy cannot be achieved only through legislation but should be embedded in the design and maintenance of information systems and operations). Article 25 codifies the principles of privacy by design and privacy by default. *Id.* In practice, the GDPR takes a flexible approach to PbD because data controllers can determine their level of compliance based on privacy risks but presents uncertainty as to the required level of compliance. *Id.*; *see also Why data security is an essential investment,* CONNECTED THINKING (Apr. 21, 2019), *archived at* https://perma.cc/2SE5-D3UK (addressing the fact that the GDPR will impose "fines for firms that don't protect data effectively—punishment could include 4% of annual turnover or 20 million euros, whichever is higher). *See* Justin Dolly, *How GDPR will affect small and midsized businesses*, CSO (May 29, 2018), *archived at* https://perma.cc/3UMT-4M3Y (stressing that non-compliance of the newly enacted GDPR will lead to penalties that are "severe for companies of all sizes"); *see also* Luke Irwin, *Does the GDPR allow you to track biometric data?,* IT GOVERNANCE (Oct. 22, 2018*), archived at* https://perma.cc/7NHK-CDSF (articulating that the GDPR has made their rules more stringent in terms of lawful processing of biometric data leading obtaining consent to be "the least preferable option").

[102] *See* Jen King, *Privacy by Design and the Uber Settlement*, CENTER FOR INTERNET AND SOCIETY (Oct. 15, 2018), *archived at* https://perma.cc/CT33-PMJX (explaining that the Uber settlement was the first time PbD requirement was ever referenced in a settlement).

[103] *See* Commercial Facial Recognition Privacy Act, S. 847, 116th Cong. (2019) (stating that the bill's purpose is to "prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user, and for other purposes"). *See Blunt, Schatz Introduce Bipartisan Commercial Facial Recognition Privacy Act*, ROY BLUNT U.S. SEN. FOR MO. (Mar. 14, 2019) [hereinafter *Blunt & Schatz Introduce Act*], *archived at* https://perma.cc/9LMQ-MSRB (highlighting that Senator Roy Blunt and Senator Brian Schatz are members of the Senate Committee on Commerce, Science, & Transportation); *see also* Chris Burt, *U.S. Congress moves to regulate facial recognition technology*, BIOMETRIC UPDATE (Mar. 15, 2019), *archived at*

The architects and supporters behind the CFRP Act hope to balance the unprecedented benefits to consumers through the use of facial recognition technology with the danger to consumer privacy if left unregulated.[104] A notable aspect of the CFRP Act is that it requires controllers to obtain explicit user consent prior to the collection of facial recognition data and it prohibits these controllers from sharing facial recognition with third parties without obtaining consumer consent.[105]

Not only does the proposed CFRP Act attempt to protect consumers from the harms of data infringement, it also intends to prohibit facial recognition technologies from being discriminatory—a harm often overlooked in the creation of these technologies.[106] In

https://perma.cc/73RW-575D (pointing out that this bill is the first step towards federal regulation of biometrics in the nation).

[104] *See Blunt & Schatz Introduce Act*, *supra* note 103 (quoting Brad Smith, President of Microsoft, "[f]acial recognition technology creates many new benefits for society and should continue to be developed, [i]ts use, however, needs to be regulated to protect against acts of bias and discrimination, preserve consumer privacy, and uphold our basic democratic freedoms"). Senator Blunt has expressed that there is mounting concern among consumers as to how their data is being collected and used, and in turn, he hopes that the bill will ensure that this technology continues to develop in a responsible manner. *Id. But see* Frank Konkel, *Facial Recognition Bill Would Ban Companies From Sharing Your Face Without Consent*, NEXTGOV (Mar. 15, 2019), *archived at* https://perma.cc/X2NA-PU3A (arguing that the proposed bill is not being accepted by the tech community because of fear that the legislation "could stifle the technology before its potential is reached" and they further note that "these applications are still in their infancy, and this legislation would limit many potential commercial applications").

[105] *See* Commercial Facial Recognition Privacy Act § 2(2) (defining a controller as a "covered entity that, alone or jointly with others, determines the purpose and means of processing of facial recognition data"). The CFRP Act requires controllers to obtain consent and provide concise notice to users that the facial recognition technology is being used. *Id. See* Marianne Kolbasuk McGee, *Bill that Changes HIPAA Passes House*, GOV. INFO. SECURITY (July 10, 2015), *archived at* https://perma.cc/XT76-P2NM (discussing the rationale behind a consent requirement).

[106] *See* Commercial Facial Recognition Privacy Act § 3(d) (urging entities to engage in "independent testing to conduct reasonable tests of the facial recognition technology for accuracy and bias"). The CFRP also prohibits entities from putting facial recognition technology on the market that may result in reasonably foreseeable material physical or financial harm or is highly offensive to the user. *Id. See* Jeffrey Neuburger, *Bipartisan Facial Recognition Privacy Bill Introduced in Congress*, PROSKAUER (Mar. 26, 2019), *archived at* https://perma.cc/Q98R-UXTT (indicating that the CFRP Act prohibits use of biometric technology for discriminatory purposes and requires third-party testing "to address accuracy and bias issues").

terms of enforcement, the CFRP Act gives the FTC and state attorney generals the right to file claims under the act.[107] Regulations for data security and retention standards are essential to protecting biometric information and the CFRP Act will give the FTC and the NIST the power to promulgate them.[108]

IV. Analysis

With the rise of entities using individuals' biometric data in their products and services, it is important that the use and retention of this data is federally protected because of the immutability of biometrics. Although some may argue that there is enough data protection through the FTC, Gramm-Leach-Bliley Act, HIPAA, and the Fair Credit Reporting Act, the salient issue is that their methods of protecting information are insufficient.[109] These pieces of legislation do not offer biometric data protection of all consumer products and services which is necessary due to the mounting integration of biometric data into consumer products.[110] Accordingly efforts should be made to federally regulate the area of biometrics; self-regulation is not sufficient.

Some states such as Illinois, Texas, and Washington have acknowledged the importance of protecting consumer's biometric information leading to the adoption of biometric legislation in their

---

[107] *See* Commercial Facial Recognition Privacy Act § 4 (allowing the FTC to enforce the Act and granting the attorney general authority to bring a civil action on behalf of the State).

[108] *See id.* § 5 (granting the FTC and the NIST the power to promulgate regulations). Outlining that the FTC can govern the limits for

> [D]escribing data security, minimization, and retention standards to be met at a minimum by processors; (2) defining what is harmful and highly offensive under paragraphs (1) and (2) of section 3(c); and (3) expanding the list of exceptions described in section 3(e) where it is impossible for a controller to obtain affirmative consent from, or provide notice to, end users.

Id.

[109] *See* Jolly, *supra* note 26 (listing the FTC, GLBA, HIPAA, and the Fair Credit Reporting Act as notable data privacy regulations).

[110] *See Biometric data and data protection regulations (GDPR & CCPA)*, *supra* note 34 (declaring that biometric information is not federally regulated but biometrics are covered in certain pieces of legislation to an extent).

respective states.[111] However, Illinois is the only state that provides a private right of action allowing citizens to assert their grievances.[112] Although the private right of action is an effective way of alleging harm, the litigation arising from BIPA has been confusing for businesses and not necessarily protecting consumers.[113] While enacting statutes to protect biometric data is a good first step, it is not enough to protect consumers from all over the nation because the statutes are only enforceable on a state specific level.[114]

The European Union's GDPR strengthens data privacy laws within the EU and with entities that do business in the EU.[115] Notably, the GDPR recognizes biometric data as a special category of personal data which leads to stronger protection.[116] The EU has also enacted Article 25, privacy by design, which forces businesses to implement effective safeguards into technology at the onset.[117] Due to the significance of biometric data, it is favorable that companies take precaution in protecting this data rather than risk the ability to do business in the EU.[118] With the impact of the GDPR on countries that do business with the EU, such as the United States, the sensible course of action would be for the United States to have federal enforcement through the FTC with guidelines that mimic the GDPR but that have less teeth to allow innovation for businesses.[119]

---

[111] *See id.* (indicating that Washington, Illinois, and Texas have state biometric privacy laws).
[112] *See* Newcombe, *supra* note 46 (indicating that BIPA has a private right of action).
[113] *See* McCray, *supra* note 46 (examining subsequent litigation under BIPA and the confusion surrounding what it means to have "harm" under the statute).
[114] *See* Schwartz, *supra* note 36 (recognizing that the Illinois BIPA is the strongest biometric law in the country).
[115] *See* Lord, *supra* note 100 (indicating that a company that does business in the EU is subject to the GDPR).
[116] *See* Irwin, *supra* note 101 (stating that the GDPR considers biometrics a special category of personal data).
[117] *See* Leentfaar, *supra* note 99 (articulating that Article 25 of the GDPR codifies the principles of privacy by design and privacy by default).
[118] *See* Glaser, *supra* note 6 (focusing on the fact that consumers should be wary about releasing their biometric data to online systems).
[119] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 48 (stressing that any controller, which could be a business, is subject to the GDPR); Lord, *supra* note 100 (highlighting that any corporation that markets their goods or services in the EU must follow the GDPR); Dolly, *supra* note 101 (stressing that small and mid-size companies will need to raise capital to update their security protocols to be in compliance with the GDPR, which may also thwart companies from venturing into data-collecting markets).

A. FTC as an (Un)Enforcer of Biometrics

The FTC has the power to enforce actions against companies who have engaged in unfair or deceptive practices, such as when companies have data breaches, which is helpful for consumers who have had their private information compromised.[120] Although the FTC has the power to enforce these suits against uncompliant companies, it has does not currently have regulation to oversee the security of biometric information.[121] At the moment, the only regulations that apply to biometric information are the policies that regulate other sensitive personal information, which is insufficient because biometric identifiers are immutable and require a higher level of protection.[122] Although, the FTC released a document on the best practices of the self-regulation of biometric information, companies can still have the power to decide whether to follow it or not, since it is unenforceable and at varying levels which is dangerous for consumers.[123] Given the sensitivity of biometric information, companies shouldn't have the sole discretion to decide when and which practices to follow, there should be a uniform standard that must be followed.

B. Biometric Statutes are Asymmetrical

Illinois, Texas, and Washington have led the movement in protection for biometric identifiers, however, the asymmetry of their respective laws makes it increasingly difficult for businesses to ascertain whether they are being complaint or not.[124] For example, the

---

[120] *See* FTC REPORT, *supra* note 30 (promulgating that the FTC has the power to bring enforcement actions when companies mishandle consumers' data).

[121] *See* FACING FACTS, *supra* note 24, at 9–10 (outlining that the FTC does not have the power to regulate biometric data but has provided guidelines on the best practices for the collection of biometric data).

[122] *See* Glaser, *supra* note 6 (discussing that biometrics are a higher class of personal information because of its immutability; an individual can't get another body part back like a password).

[123] *See* FACING FACTS, *supra* note 24, at iii (setting forth that the best practices are not enforceable, but rather is a manner in which companies should regulate their security systems and provide notice to consumers).

[124] *Compare* BIPA § 15(b) (adopting regulations stating that consumers should be given notice and companies should obtain consent in the collection and capture of biometric identifiers), *and* TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017)

simple definition for a biometric identifier or biometric information is different across the board, with some having exclusions and some not.[125] Due to the lack of uniformity in the plain definition of a biometric identifier or information, businesses may be compliant in one state but not in the other, making it very difficult for companies to test out new products and services in the market without the risk of a fine.[126]

BIPA notably has a private right of action within its statute, which on its face provides consumers with the power to enforce their grievances.[127] However, the case law that has followed from it has been unfavorable for businesses and not necessarily more secure for consumers.[128] On the other hand, H.B. 1493 and B.C. 503.001 do not have a private right of action within their statutes, giving the attorney general the discretion to enforce the statute.[129] Given that the attorney general is the sole enforcer, it is likely that actions won't be brought forward until something such as a breach occurs, which at that point

(mandating that entities obtain consent in the collection and capture of biometric identifiers), *with* WASH. REV. CODE § 40.26.020 (2019) (articulating that entities only need to provide notice and consent for the collection of biometric data, not the capture).

[125] *See* BIPA § 10 (defining a biometric identifier as a retina or iris scan, fingerprint, voiceprint or a scan of hand or face geometry and having exclusions to the definition of a biometric identifier); *see also* WASH. REV. CODE § 40.26.020 (2019) (defining a biometric identifier as an automatic measurement of an individual's biological characteristics in the form of data); BUS. & COM. § 503.001 (describing a biometric identifier as a retina or iris scan, fingerprint, or record of hand or face geometry but does not share exclusions like BIPA does); Kohne et al., *supra* note 39 (questioning whether information derived from a photograph is a biometric identifier under BIPA and B.C. 503.001).

[126] *See* Kohne et al., *supra* note 39 (evaluating that the current statutory framework is causing uncertainty). The authors opine on a decision that granted a plaintiff relief for a company using her photograph to identify the plaintiff's face pattern). "[T]he decision puts: (1) further uncertainty in BIPA's definition of biometric information; (2) companies at risk for suit; and (3) consumers' biometric information at risk." *Id.*

[127] *See Sensitive to the Touch*, *supra* note 58 (discussing how BIPA is the only state where courts are permitted "enforce biometric laws for consumer-claimants").

[128] *See* BIPA § 20 (granting individuals a private right of action); *see* Rosenbach v. Six Flags Entm't Corp. (*Rosenbach II*), 129 N.E.3d 1197, 1206–07 (Ill. 2019) (holding that companies who violate a procedural aspect of the statute will be subject to a cause of action).

[129] *See* Wash. H.B. 1493 (permitting the attorney general to enforce actions against companies who violate the statute); *see also* BUS. & COM. § 503.001 (barring individuals from bringing an action against companies that violate the statute by stating that the attorney general may bring an action for recovery).

there isn't really a proper recourse for consumers.[130] Conversely, individuals under BIPA have brought claims forward preemptively, stating claims for lack of notice, rather than a breach.[131] With regards to biometric data, it is better to have a preemptive claim rather than waiting for a breach of this information to occur, so a private right of action is preferable, but there needs to be limitations to it as discussed below.

All of these statutes have limitations on the commercial use of biometric identifiers, with some being stronger than others. BIPA, being the strongest, outlines that a private entity cannot collect or capture a biometric identifier without providing notice and obtaining consumer consent making it mandatory for entities to inform the consumer even if they are not storing any biometric information.[132] B.C 503.001 also requires companies to obtain consent prior to capturing a biometric identifier, but the difference from BIPA is that the two states have different definitions for biometric identifiers and biometric information, so what exactly must be given notice prior to capture is slightly distinct.[133] H.B. 1493 diverges from the aforementioned because companies do not have to provide any notice or get consent if they are simply capturing a biometric identifier, making it easier for companies to use biometric identifiers in a one-time transaction without requesting consent each time. However, it also incentivizes companies to disregard security protocol if the biometric identifier is only being used for a limited time and then being

[130] *See* Gartland, *supra* note 3 (stressing the privacy and security concerns with breach of biometric data by arguing that "it's possible to replace a stolen credit card or bank account number, but how do you replace fingerprints, facial features or an iris…instead of credit monitoring, will hacked companies offer their customers plastic surgery?").

[131] *See Rosenbach II*, 129 N.E.3d 1197 (reviewing action for collection of biometric identifiers without notice or consent); *see also* Rivera v. Google Inc. (*Rivera II*), 366 F. Supp. 3d 998, 1001 (N.D. Ill. 2018) (claiming damages for the collection of facial biometric identifiers without notice or consent).

[132] *See* Schwartz, *supra* note 36 (claiming that BIPA offers the strongest protections for consumers).

[133] *See* BIPA § 10 (providing a definition for biometric information); *see also* BUS. & COM. § 503.001 (creating a definition for biometric identifiers but not biometric information); 2017 Wash. Sess. Laws 457 (addressing biometric identifiers but not biometric information).

destroyed.[134] While providing notice and obtaining consent is important, in certain transactions it can be inconvenient and unnecessary, and may not even necessarily protect a person's biometric information.[135] Overall, the most stringent regulation on collection of biometric identifiers or information is BIPA, while the most flexible is H.B. 1493.

C. The Application of BIPA is Confusing and Inconsistent

Rosenbach v. Six Flags,[136] *Rivera v. Google*,[137] and *In re Facebook*,[138] are cases that have been considered monumental in this field in discerning the level of protection that an individual deserves regarding their privacy.[139] When BIPA construes an "aggrieved" person to be one that has suffered a technical violation of the statute, the consumer is essentially guaranteed to receive damages.[140] In *Rosenbach*, the court analyzed whether an individual that had their biometric identifier collected without notice or consent could be considered an "aggrieved" person under the statute deserving of

[134] *See* FACING FACTS, *supra* note 24, at 14, 17 (guiding entities to store information captured in the form of statistics to reduce the risk that the data will be tied to a particular person and also recommends implementing reasonable security measures while the biometric identifier is in possession).

[135] *See* FACING FACTS, *supra* note 24, at 15–16 (promulgating a sliding scale of notice and choice and supports a "walk away choice" since the security implications are low in the situation where technology does not store images or biometric identifiers). A walk away choice is when an entity places a sign indicating that the technology used in that particular area has facial recognition technology, and consumers can decide whether to go into that area or walk away. *Id.* at 15. However, some panelists believe that this is not fair for consumers who want to enter a specific area but also do not want to be recognized by facial technology. *Id.*

[136] No. 2-17-0317, 2017 WL 6523910 (Ill. App. Ct. Dec. 21, 2017). This case was further appealed to the Illinois Supreme Court. *See* Rosenbach v. Six Flags Entm't Corp. (*Rosenbach II*), 129 N.E.3d 1197 (Ill. 2019).

[137] 238 F. Supp. 3d 1088.

[138] 326 F.R.D. 535.

[139] *See* McCray, *supra* note 46 (discussing that while biometric data has led to increased convenience and efficiency for users it has resulted in a flood if legislation and litigation to determine how this nontraditional data will be managed).

[140] *See* Bologna, *supra* note 72 (arguing that there will be an increase of cases brought under BIPA if an aggrieved person is one who's suffered a technical violation of statute).

damages.[141] On appeal in 2019, the Illinois Supreme Court held that a person who suffered a technical violation of their rights, not an actual harm, under the act is deserving of the damages offered under BIPA.[142] In sum, the holding of the *Rosenbach* court has opened the doors for litigants to assert relief in state court for situations where a company has not given proper notice and consent.[143] When going before a federal court, defendants will be able to assert the Article III defense exposing the flaw with BIPA's statute, that standing will continue to be an issue hindering plaintiffs from protecting their privacy rights on the federal level.[144] Although this will make companies more conscientious of updating their privacy policies, it does not necessarily incentivize these companies to increase their security protocol when the identifiers are in their possession.[145]

More recently, the district court stipulated in *In re Facebook* that the 2017 *Rosenbach* holding does not dominate and that a correct interpretation would be that injury to a privacy right is enough to be an aggrieved person under BIPA.[146] Since *Rosenbach* has adopted this interpretation in the Illinois Supreme Court, it has diminished the

[141] *See Rosenbach I*, 2017 WL 6523910 (advocating for a narrow definition of BIPA to apply only in cases where there was the occurrence of an injury from the use of the biometric data and not merely a technical violation).

[142] *See Rosenbach II*, 129 N.E.3d 1197 (holding that a technical violation is enough for a plaintiff to obtain damages).

[143] *See* Chan, *supra* note 75 (alleging that the holding will lead to an influx of claims in the docket of state courts).

[144] *See* Kracht et al., *supra* note 83 (discussing that there has been difficulty by the federal courts to ascertain whether the improper collection of biometric data is a concreate harm giving defendants the opportunity to "successfully argue that violations of BIPA's notice and consent procedures do not present sufficient risk of harm in every case").

[145] *See* Fleishman, *supra* note 31 (criticizing Equifax for its failure to use "well-known security practices and a lack of internal controls and routine security reviews" and for only creating a budget for the enhancement of its security systems after being imposed consent orders from eight state banking regulators). Equifax may have had privacy policies in place, yet that did not preclude them from being neglectful of their security practices and failing to use encryption to protect sensitive personal data. *Id.*

[146] *See In re Facebook*, 326 F.R.D. at 545 (holding that an actual harm is not necessary to have a violation under BIPA and that a violation of a privacy right is sufficient to be aggrieved under BIPA). The court stipulated that the invasion of a legal right means that a person is aggrieved. *Id.*

defense of lack of Article III standing because now the statutory violation is an injury-in-fact.[147] As noted before, this should logically lead to stronger compliance with consent and notice requirements in place.[148]

In sharp contrast, *Rivera* has curtailed the ability of litigants to assert relief in federal court because the court held that a technical violation of the statute is not a concrete harm deserving of Article III standing.[149] In *Rivera*, Google collected individuals' face geometry by creating a face template from a photograph.[150] The district court's holding failed to acknowledge the legislative intent in enacting BIPA and disregards the protection of individuals' biometric data at collection.[151] The outcome of the case allows defendants to use lack of Article III standing as a defense in federal court and fails to address the issues with regulating emerging technologies that hinge on an individual's privacy rights.[152] The court also expanded the definition of biometric identifiers and information by stating that a photograph could be considered biometric information, even though in the statute it is excluded, making it more difficult for businesses to determine whether they are being compliant with BIPA.[153]

---

[147] *See* Kennerly, *supra* note 83 (setting forth that plaintiffs failed to show an injury-in-fact sufficient to confer Article III standing).

[148] *See* Rosenblatt, *supra* note 87 (discussing the judge's statement that "this injury is worlds away from the trivial harm of a mishandled zip code or credit card receipt").

[149] *See* Rivera v. Google Inc. (*Rivera II*), 366 F. Supp. 3d 998, 1007 (N.D. Ill. 2018) (holding that a technical violation is not concrete enough to be considered an actual harm worthy of Article III standing, it is not enough that the litigant fears that their privacy rights will be infringed).

[150] *See id.* at 1090 (contending that defendant infringed on privacy rights by making facial scans of their photographs and measuring their biological measurements therefrom).

[151] *See* Goldman, *supra* note 83 (arguing that although BIPA's legislative findings discussed that biometrics were immutable and could not be easily changed, there was also a suggestion that harm only results from disclosure not from its mere collection).

[152] *See Rivera*, 366 F. Supp. 3d at 1001 (setting forth that plaintiffs failed to show an injury-in-fact sufficient to confer Article III standing). In its concluding remarks, it also noted that the case presented close legal questions, which are "not uncommon when it comes to technological advances." *Id.* It cautioned that "[t]he difficulty in predicting technological advances and their legal effects is one reason why legislative pronouncements with minimum statutory damages and fee-shifting might reasonably be considered a too-blunt instrument for dealing with technology." *Id.* at 1013 n.20.

[153] *See id.* at 1095 (exploring that the statute's definition of biometric information lends support for the court's interpretation of a photograph being considered a

D. Proposed Regulation

The omnipresence of biometric information is inevitable.[154] With it, consumers should be able to feel secure about their privacy, and companies should have the freedom to innovate and integrate.[155] The most effective resolution between these competing interests is federal regulation that encompasses the FTC's guidelines, parts of the biometric statutes, the newly introduced CFRPA and the GDPR's privacy by design mandate.

1. Notice and Consent

It is important for consumers to be well-informed as to what is occurring with their biometric information, yet there must be a balance between protecting consumer's privacy rights and supporting innovation.[156] In terms of giving notice and obtaining consent, it is advisable to follow the Washington H.B. 1493 regulation on notice and consent because it provides flexibility and convenience to businesses using biometric identifiers for one-time use, but also places more stringent notice and consent guidelines on companies that are storing this information. Along with adhering to the Washington H.B. 1493 regulation, federal regulation should also incorporate some guidelines from the CFPR.[157] All of the state biometric statutes and the CFPR contain regulation concerning third-party information sharing, and that

biometric identifier). However, a photograph will only be considered a biometric identifier if an entity derives biological measurements therefrom. *Id* at 1097.

[154] *See Blunt & Schatz Introduce Act*, *supra* note 103 (stressing that the development of facial recognition technology is expanding in the commercial sector). Although facial recognition technology has become increasingly more prevalent, many consumers are unfamiliar to its omnipresence. *Id.*

[155] *See* Gartland, *supra* note 3 (arguing for the protections of consumers in that they are "not be left powerless against profound threats to privacy and . . . security").

[156] *See* FACING FACTS, *supra* note 24 (inferring that the FTC promulgated privacy by design in conjunction with notice and consent because it thought necessary that this kind of information have a wide variety of methods to protect biometric privacy).

[157] *See* Commercial Facial Recognition Privacy Act, S. 847, 116th Cong. §3(a)(1)(B)(i) (2019) (providing that the consumer must be given notice of the presence of facial technology). A consumer must also be given information on the capabilities and limitations of the facial recognition technology in place. *Id.* § 3(a)(1)(B)(ii).

practice should be continued to inform consumers and give them control over their biometric information.[158] In terms of the disclosure, sale, and lease of biometric information, the Washington H.B. 1493 should be followed because it only applies to the collection of biometric information, most at risk for being sold to other parties, and it provides consumers with relevant information when their information is being used for another purpose.[159]

2. Destruction Cycle

In terms of destruction cycles of biometric identifiers, the Texas B.C. 503.001 should be followed because it contains the shortest retention cycle for biometric identifiers, minimizing the risk that biometric identifiers will be compromised and ensures that they are only being used for the company's intended purpose.[160] Where the CFPR fails is that it doesn't outline a specific destruction cycle of biometric identifiers, instead, it outlines that consumers should be given information on the deletion process.[161] While being given the deletion process is helpful, it is more helpful for consumers to have a guaranteed time period as to when their biometric information will be deleted from a company.[162]

[158] *See id.* § 3(a)(4) (outlining that a controller cannot repurpose facial recognition data for a different purpose and controllers cannot share facial recognition data "with an unaffiliated third party without affirmative consent").
[159] *See* H.R. 1493, 65th Leg., 1st Reg. Sess. (Wash. 2017) (requiring notice and consent in situations where biometric identifiers are being collected, but not when biometric identifiers are being merely captured for a commercial purpose).
[160] *See* TEX. BUS. & COM. CODE § 503.001 (West 2017) (explaining that entities must destroy biometric identifiers a year after the purpose for it has ended); *see also* Browning, *supra* note 66, at 676 (evaluating that out of all of the biometric statutes, Texas has a more accelerated destruction rate of biometric identifiers).
[161] *See* Commercial Facial Recognition Privacy Act § 3(b)(1) (2019) (mandating that consumers are given information on the deletion process so that they can give informed consent).
[162] *See* BUS. & COM. § 503.001 (implying that possessor of biometric identifier has at most one year to delete information after it is no longer required to be maintained by law).

3. Biometric Identifier Definition

Rivera v. Google[163] complicated interpreting the definition of a biometric identifier under BIPA, leading to unclear results for businesses whom are under the impression that they are being compliant.[164] However, the BIPA definition of a biometric identifier and biometric information is the most comprehensive and detailed so it should be used, but there should be more information in the regulation concerning photographs.[165] However, the newly introduced CFPR gives the most detailed definition for facial recognition data and should be followed to mitigate confusion for companies.[166] More specifically, analogously to BIPA's definition of biometric identifier and information, the CFPR separates the definition of facial information into facial recognition technology and facial recognition data.[167]

4. Security

The proposed federal regulation makes providing notice and obtaining consent more flexible, but in terms of the security of these biometric identifiers, federal regulation should draw inspiration from the GDPR's privacy by design mandate.[168] Most data breaches that

---

[163] 238 F. Supp. 3d 1088 (N.D. Ill. 2017); 366 F. Supp. 3d 998, 1001 (N.D. Ill. 2018).
[164] *See Rivera I*, 238 F. Supp. 3d at 1092 (holding that although photographs are excluded from biometric identifiers, the court presumed it was biometric information because biological measurements were derived from photographs).
[165] *See* BIPA § 10 (granting a definition for biometric identifier and biometric information, while also including exclusions for biometric identifiers).
[166] *See* Commercial Facial Recognition Privacy Act, S. 847, 116th Cong. § 2(5) (2019) (providing a definition for facial recognition technology). The CFRP Act defines facial recognition technology as technology that "(A) analyzes facial features in still or video images; and (B) (i) is used to assign a unique, persistent identifier; or (ii) is used for the unique personal identification of a specific individual." *Id.*
[167] *See id.* §§ 2(5)–(6) (distinguishing facial recognition technology from facial recognition data). Facial recognition data is defined as "any unique attribute or feature of the face of an end user that is used by facial recognition technology to assign a unique, persistent identifier or for the unique personal identification of a specific individual." *Id.* § 2(6).
[168] *See GDPR & CCPA*, *supra* note 34 (suggesting data usage should be limited to whatever is necessary).

arise with other sensitive personal information occurs because of the implementation of vulnerable security systems; and this practice should not be continued with biometric information.[169] Privacy by design proponents encourage implementing secure practices in every stage of product and service development, and it makes sense to follow this standard because an individual's privacy rights are truly harmed when this data is compromised.[170] For example, when biometric information is being collected, companies should implement encryption into these systems to effectively protect this information and prevent hacking.[171] On the other hand, when biometric information is being merely captured, companies should implement the strongest protections in the industry to prevent hacking from occurring while the company is in possession of biometric identifiers.[172] To incentivize stronger security systems for biometric systems, and to avoid companies disregarding the statute, significantly larger penalties for inadequate security systems should be imposed to companies.[173] In making notice and consent more flexible and strengthening the regulation of the security systems containing biometric information, there is more of an incentive for companies to

[169] *See* Fleishman, *supra* note 31 (describing that the Equifax breach occurred because of poor data security practices).

[170] *See id.* (recalling that the data breach caused people's personal information such as social security, passwords, addresses, and credit card numbers to be compromised and exposed them to a risk of fraud and identity theft).

[171] *See Knox Platform for Enterprise: Root of Trust*, *supra* note 24 (noting that Samsung uses encryption to protect its devices through securing its hardware and software systems); *see also About Face ID advanced technology*, *supra* note 24 (stating that Apple uses encryption to protect an individual's biometric information from hackers and that the consumer only has access and the right to destroy this data).

[172] *See* FACING FACTS, *supra* note 24, at 2 (reasoning that in the case of collection, companies should implement strong security protections for images and for the biometric information collected from the images). Many of the panelists stressed the importance of data security measures and suggested encryption of the biometric information. *Id.* at 17.

[173] *See Why data security is an essential investment*, *supra* note 101 (advising that the GDPR's steep fines for ineffective data security is the driver for the enhancement of security systems). The Vice President of Innovation labs opines that "it's a shame that regulatory change and threats of fine are the catalyst, but in some cases that's what it takes, and any resulting investment and improvement will benefit companies in the longer term." *Id.*

focus on protecting individuals from the unlawful breach of biometric information the undeniable true harm to their privacy rights.[174]

V. Conclusion

The omnipresence of biometric information being incorporated into biometric technology is exciting, but it comes with serious privacy and security concerns. It is not surprising that there is a lack of federal regulation due to its novelty in the field of consumer products and services, but this should not deter the legislature from being proactive in ensuring the security and privacy of individuals. There are problems with having each state enact its own biometric legislation because it is not favorable for companies who want to innovate and make their products more convenient for users since it would require companies to be focused on compliance with each statute. Although compliance with statute is obviously preferable, it is not business-friendly, nor does it necessarily protect consumers because it puts too much focus on having privacy policies that are compliant to each state rather than focusing on the real security issue.

This Note therefore suggests implementation of federal regulation that provides a right of action like BIPA, because suits will only arise for the improper collection—not mere capture—of biometric information incentivizing companies that are collecting to update their privacy policies accordingly if they are in possession of biometric identifiers. In terms of unlawful disclosure, the FTC should be the sole enforcer, giving out larger fines if it's due to a security breach and lower fines if the company failed to obtain consent. Even more, the FTC should regulate and give out fines for companies that are non-compliant with the privacy by design mandate. Giving the FTC the power of enforcement provides consumers with more protection and incentivizes companies to exercise their due diligence to avoid fines and lawsuits from the FTC. This proposal takes into consideration the importance of having an informed consumer, but addresses the real issue with biometric information, which is mandating secure data systems containing this sensitive information.

[174] *See* McGee, *supra* note 105 (discussing how allowing the use of PHI without consent hinders the privacy and security of that data and makes it less certain).