NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 19, ONLINE: APRIL 2018

FINGERPRINT NOT RECOGNIZED: WHY THE UNITED STATES NEEDS TO PROTECT BIOMETRIC PRIVACY

Blake Benson*

Rising interest in biometrics—the modern umbrella term for physical and behavioral characteristics possessed by humans and used to identify one another—has motivated large technology companies to produce products that allow consumers to access vital information using only their unique biometric identifiers. Because biometric information is unique to each person on the planet, it is a valuable way to secure personal data. However, the uniqueness and permanence of biometric information heighten the consequences of security breaches when compared to the compromise of simple alphanumeric passwords. Growing interest in biometric technology across the United States has motivated a small number of state legislatures to address the collection, storage, and distribution of biometric information by business entities, but the legal framework for handling that information is largely underdeveloped. As biometric identification becomes more prevalent, the rest of the states and the federal government must decide how to address privacy concerns. Passing new laws, retrofitting old laws to address new technologies, and choosing not to take legislative action are just a few of the options both state and federal governments are considering. Based on the level of interest, and the number of concerns, with biometric identification technology, the federal government is best equipped to address these concerns. If Congress chooses to introduce biometric privacy legislation, which would provide uniform protection for all American consumers and employees, there will certainly be relentless lobbying from the tech

* J.D. Candidate, University of North Carolina School of Law, 2019. The author would like to thank the staff and editors of the UNC Journal of Law & Technology for their contributions to this Recent Development. The author would specifically like to thank Editor-in-Chief Erin Larson, Executive Editors Joseph Hjelt & Jordan Luebkemann, and Notes Editors Christopher Burks & Amy Leitner for their advice and hard work throughout the publication process.

sector concerning the contents of the bill. Congress will need to balance biometric privacy with corporate interests if they decide to try and enact a much-needed biometric privacy law.

I. INTRODUCTION

Humans have been using physical and behavioral traits, or biometrics, to identify one another for thousands of years.[1] Biometrics are officially defined as "measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity" by the Biometric Research Group.[2] Ancient Egyptians used physical characteristics to differentiate between trustworthy and untrustworthy traders, while the Babylonians verified business transactions by stamping fingerprints into clay tablets as early as the sixth century.[3] By the nineteenth century, societies used physical characteristics, such as height, arm length, and fingerprints, to document convicted criminals and identify suspects in ongoing criminal investigations.[4] Modern technology has made cataloging and using physical characteristics for various purposes far easier and more expansive.[5] Today, using biometrics to identify someone is just another part of daily life.[6] For example, modern smartphones offer users the option of unlocking their device with a fingerprint before they log in to their Facebook application and use its facial recognition function to tag friends in photos.[7] Technology has made physical biometric identification a valuable, and readily available, tool for countless people across the globe.[8]

Commercial use of biometric technology has become particularly divisive in the United States. A 2017 study conducted by Viewpost, an American corporation offering online payment

---

[1] *See* Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE (Jan. 14, 2015), http://www.biometricupdate.com/201501/history-of-biometrics.

[2] Rawlson King, *What Are Biometrics?*, BIOMETRIC UPDATE (Jan. 24, 2016), http://www.biometricupdate.com/201601/what-are-biometrics-2.

[3] Silvio Barra et al., *Unconstrained Ear Processing: What Is Possible and What Must Be Done*, *in* SIGNAL AND IMAGE PROCESSING FOR BIOMETRICS 130 (Jason Scharcanski et al. eds., 2014); Mayhew, *supra* note 1.

[4] Mayhew, *supra* note 1.

[5] *See generally* April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.

[6] *See id*.

[7] *See id*.

[8] *See id*.

services, found that 80% of the 1,000 Americans surveyed are "in support of biometrics-enabled payments technologies and currencies" and that 50% "believe fingerprint technology will be used for authentication to pay and receive payments over the next 10 years."[9] A conflicting study prepared by the Consumer Technology Association (CTA) in March of 2016 reported that 28% of American adults are "less than comfortable" and another 42% "have neutral sentiments" about the usage of biometric technology for commercial purposes.[10] Yet another survey, conducted by the information technology corporation Unisys, determined that 33% of the 11,244 Americans surveyed actually thought biometric identifiers were "effective security feature[s]."[11] Conflicting survey results seem to indicate that commercial use of biometric technology has divided Americans into two categories: those that are willing to sacrifice their right to privacy for efficient, accurate biometric identification features and those that are not. Of course, it is possible that the survey results referenced may be skewed by questions that emphasize either privacy or innovation. Biometric identification features offer improved convenience and accuracy to consumers, but a large number of Americans are not willing to sacrifice the privacy of their unique identifiers for the ability to log into their bank account with a fingerprint instead of an alphanumeric password.[12]

Biometric technology offers Americans a vast array of benefits, but they come at a cost.[13] Biometric information is both "inherently public," meaning that other people can easily view and gain access

---

[9] Justin Lee, *Study Finds Americans Support Biometrics-based Payment Systems*, BIOMETRIC UPDATE (July 18, 2017), http://www.biometricupdate.com/201707/study-finds-americans-support-biometrics-based-payment-systems.

[10] *Recent Opinion Surveys on Public Perceptions of Biometrics*, INT'L BIOMETRICS & IDENTITY ASS'N, https://www.ibia.org/download/datasets/3372/Public-Perceptions-of-Biometrics-opinion-surveys%20.pdf.

[11] Justin Lee, *Unisys Survey Finds One-third of Americans View Biometrics on Smartphones as Effective*, BIOMETRIC UPDATE (July 6, 2015), http://www.biometricupdate.com/201507/unisys-survey-finds-one-third-of-americans-view-biometrics-on-smartphones-as-effective.

[12] *See* Glaser, *supra* note 5.

[13] *See id.* (telling readers that biometrics are beneficial to Americans but that they also have many drawbacks that must be properly mitigated).

to it, and "inherently private" because every American possesses unique biometric identifiers.[14] Unlike a password, which is designed to be kept secret and can be changed in seconds, biometric information is permanent, making it extremely sensitive material.[15] Just one example of this privacy concern is how often American's leave fingerprints on different surfaces.[16] The inherently public nature of biometrics leads to another pressing issue: the collection and usage of biometric information by businesses, law enforcement officials, and other third parties.[17] Facebook's opt-in facial recognition feature is one example of a third-party using the inherently public nature of biometrics for a proprietary purpose.[18] Third-party usage of biometrics does not stop at physical characteristics either: Israeli firm BioCatch is developing a technology to track computer usage behavior for detection of fraudulent banking and shopping activity.[19] Biometric technology can make daily activities, like logging into a phone, easier and more secure, but there are obvious concerns that must be addressed because biometric identifiers can be classified as both public and private information.[20]

Although state governments have taken notice of the rising number of corporations investing in biometric technology, few states have actually taken action to mitigate the negative impacts of

---

[14] *See id*.

[15] *See* Chiara A. Sottile, *As Biometric Scanning Use Grows, So Does Security Risk*, NBC (July 24, 2016, 7:29 PM), https://www.nbcnews.com/mach/mach/biometric-scanning-use-grows-so-do-security-risks-ncna593161 (explaining that biometric data breaches are extremely severe because identifiers are unique to each individual and cannot be changed if the information is stolen or disseminated).

[16] *See* Glaser, *supra* note 5 (explaining that finger prints are left on everyday objects, like glassware, and businesses interested in acquiring those prints can do so with relative ease if they so choose).

[17] *See id.* (establishing that other government entities, like the IRS, hospitals, and banks, are third parties that use biometric identification technology).

[18] Stuart Dredge, *10 Things You Need to Know About Biometrics Technology*, THE GUARDIAN (Sept. 17, 2014), https://www.theguardian.com/technology/2014/sep/17/10-things-to-know-about-biometrics.

[19] *Id*.

[20] *See* Glaser, *supra* note 5.

the technology on individual privacy.[21] Illinois, Washington, and Texas are currently the only states that have enacted commercial biometric privacy laws.[22] As of the publication date of this Recent Development, no federal efforts to pass a commercial biometric privacy law have been reported. Other states have biometric privacy laws pending, and Montana is all but certain to pass its own biometric privacy law this year.[23] The existing laws in Illinois, Washington, and Texas impose civil penalties for violations, but only the Illinois law offers citizens a private right of action.[24] Washington and Texas's commercial biometric privacy laws leave enforcement up to the state's attorney general.[25] As more states decide whether to protect their citizens' biometric privacy, the question of whether the federal government should step in and pass a law regulating the collection of biometrics on a national scale becomes increasingly relevant.

This Recent Development advocates for a much-needed federal law that protects consumers and employees from identity theft stemming from the improper or negligent commercial usage of biometric information. It is important for this law to include a private right of action so citizens themselves can hold commercial entities responsible for potential misuses of biometric information. A federal law offering citizens a private right of action will have drawbacks, including staunch opposition from tech companies and numerous courtroom battles over statutory interpretation. Most new laws require some level of interpretation,[26] but a biometric privacy law would be particularly troublesome because there is no

---

[21] Karla Grossenbacher & Christopher W. Kelleher, *Hazards Ahead: Uptick in Biometric Privacy Laws Can Put Employers in Hot Seat*, EMP. L. LOOKOUT (Oct. 3, 2017), https://www.laborandemploymentlawcounsel.com/2017/10/hazards-ahead-uptick-in-biometric-privacy-laws-can-put-employers-in-hot-seat/.

[22] 740 ILL. COMP. STAT. 14/10 (2008); 11 TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009); H.B. 1493, 65th Leg. Reg. Sess. (Wash. 2017).

[23] *See* Grossenbacher & Kelleher, *supra* note 21.

[24] *See* COMP. STAT. 14/10; BUS. & COM. § 503.001; H.B. 1493 (Wash. 2017).

[25] *See* BUS. & COM. § 503.001; H.B. 1493 (Wash. 2017).

[26] *See generally* LARRY M. EIG, CONG. RESEARCH SERV., 97-589, STATUTORY INTERPRETATION: GENERAL PRINCIPLES AND RECENT TRENDS (2014) (establishing that American courts frequently need to interpret statutes when applying them to specific cases).

universally accepted set of definitions for biometric identifiers. Even a thorough definitions section will not be able to predict every application of biometric technology in the future.[27]

Current and future uses for biometric technology, as well as the policy behind why these uses demand a high-level of privacy protection, appear in Part II of this Recent Development. Part III discusses the current landscape of state biometric privacy regulations in more detail and explains why existing laws do not provide adequate protection for biometric privacy. Part IV makes recommendations on what a federal biometrics law could, and should, look like. Finally, Part V evaluates the arguments for and against enacting a federal biometric privacy law before concluding that a federal law is necessary.

II. WHY BIOMETRIC PRIVACY MATTERS

As more companies develop products that utilize biometric technology, privacy continues to become an increasingly important consideration.[28] Technology companies began releasing biometric security devices for computers in the 1990s, but early versions did not attract customers because they were "clunky" and "inconvenient."[29] Motorola released the first smartphone with a fingerprint scanner in 2011, but Apple's addition of scanners to the iPhone in 2013 ignited mainstream interest in commercial biometric technology.[30] Some privacy experts have argued, and continue to

---

[27] *See* Lara Tumeh, *Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law*, BLOOMBERG BNA (Oct. 16, 2017), https://www.jdsupra.com/legalnews/washington-s-new-biometric-privacy-70894/ (showing that even states with existing biometric privacy laws use different definitions for "biometric identifier").

[28] *See generally* Glaser, *supra* note 5 (discussing the growing usage of biometric technology in the United States and identifying the serious harm that could result from the misuse of biometric information).

[29] *See* Jack M. Germain, *IBM Introducing Fingerprint Reader into Laptop*, TECH NEWS WORLD (Oct. 4, 2004, 4:44 AM), https://www.technewsworld.com/story/37017.html (reporting that IBM introduced one of the first built-in fingerprint scanners for computers and establishing that early biometric security technology was not practical or popular).

[30] *See* Glaser, *supra* note 5 (highlighting other types of biometric technology in development including, but not limited to, heartbeat identification, speech pattern

argue, that the inherent privacy of biometric information makes it safer than alternatives like a PIN number or a user-generated password.[31] After all, these proponents assert, individual physical characteristics, like fingerprints, appear to be unique and incapable of duplication.[32]

However, Georgetown Law professor Alvaro Bedoya, the executive director of the school's Center on Privacy & Technology, argues that biometric information is not as "inherently private" as proponents want to think, and to the contrary, is actually inherently public.[33] He points out that even though each American has unique biometric information, accessing that information is as easy as taking a picture of someone's facial features or taking fingerprints off of a glass after having a drink.[34] While it is easy to notice another person's biometric identifiers, like fingerprints, those identifiers are still extremely private information unique to each individual. Biometric identifiers, like fingerprints and facial structure, are what makes each human being unique and deeming that information to be solely public conveys to the world that biometric information should be treated as a public resource. Classifying biometric identifiers as solely public information jeopardizes the biometric privacy of every American and this classification should be rejected in favor of one that emphasizes the private and public characteristics of biometric information.

Bedoya's assertion that biometric identifiers are "inherently public" is difficult to reconcile with the idea that those same identifiers should be treated as highly sensitive information, but his concerns about the misuse of biometrics are far from hypothetical.

---

identification, and even vascular eye pattern identification); Casey Newton, *Apple's New iPhone Will Read Your Fingerprint*, VERGE (Sept. 10, 2013, 1:57 PM), https://www.theverge.com/2013/9/10/4715372/confirmed-apple-iphone-5s-will-include-touch-id-fingerprint-scanner.

[31] *See* Glaser, *supra* note 5 (explaining that even though biometric technology is safer than traditional alphanumeric passwords in that it uses characteristics unique to each American, that same uniqueness makes biometrics more harmful if compromised due to one's ability to document another's biometric information).

[32] *See id*.

[33] *Id*.

[34] *Id*.

Bedoya's concerns were confirmed when Jason Chaikin, the president of a corporation that produces finger scanning technology, used Play-Doh to preserve a tester's fingerprints and unlock an iPhone at a demonstration.[35] Chaikin also managed to use the same process to unlock a Samsung Galaxy and an LG Nexus in a matter of minutes.[36] Nathaniel Couper-Noles of Neohapsis, a security firm owned by Cisco, has even handled situations where fingerprints were stolen by taking high-quality photographs without any physical replication.[37] Biometric information may be unique to each individual, but that does not make it completely secure.

The inherent and permanent uniqueness of biometric information makes it more harmful if compromised than traditional security mechanisms, such as a simple alphanumeric password.[38] Passwords and credit cards "can be easily replaced," but "it is very difficult . . . for any individual to disassociate oneself from one's biometric [information]."[39] Biometric information linked to an individual in a database is exceedingly difficult to replace or change because it is unique to that person.[40] That being said, a rare set of exceptional circumstances can change an individual's biometric identifiers.[41] More alarming, catalogs of biometric information stored on a computer database can be easily compromised in the same way as any other computer system.[42] Acquiring someone's biometric information could be as simple as acquiring an

[35] Jeff John Roberts, *This Guy Unlocked My iPhone with Play-Doh*, FORTUNE (Apr. 7, 2016), http://fortune.com/2016/04/07/guy-unlocked-iphone-play-doh/.

[36] *Id*.

[37] *Id*.

[38] *See* Glaser, *supra* note 5 (explaining that traditional identification methods can easily be changed and replaced, whereas biometrics stay unique to a single person forever).

[39] Rigoberto Chinchilla, *Ethical and Social Consequences of Biometric Technologies*, AM. SOC'Y FOR ENGINEERING EDUC. 1, 5–6 (2012), https://www.asee.org/public/conferences/8/papers/3789/view.

[40] *Id*.

[41] *See* Kaveh Waddell, *When Fingerprints Are as Easy to Steal as Passwords*, THE ATLANTIC (Mar. 24, 2017), https://www.theatlantic.com/technology/archive/2017/03/new-biometrics/520695/ (explaining that bodily changes, such as blood vessel alteration, stemming from pregnancy can confuse biometric identification technology).

[42] Chinchilla, *supra* note 39, at 5–6.

alphanumeric password once databases are created.[43] The same unique characteristics that make biometric identification technology so appealing also make mitigating compromised data considerably more difficult than resetting a stolen password.[44]

III. THE CURRENT LANDSCAPE OF AMERICAN BIOMETRIC PRIVACY LAW

A select number of state legislatures have introduced or passed biometric privacy laws in response to the rising number of commercial products that offer biometric recognition.[45] Illinois passed the Biometric Information Privacy Act in 2008, making it the first state with a commercial biometric privacy law.[46] Texas followed Illinois's lead and became the second state to enact a biometric privacy law in 2009,[47] while Washington became the third state when it passed H.B. 1493 in May 2017.[48] No other states have joined Illinois, Texas, and Washington, but biometric privacy laws are pending in Massachusetts and New Hampshire.[49] At the time of publication, Congress has not taken public steps towards a nationwide biometric privacy law.

Although state governments are just beginning to regulate commercial collection of biometric information, they have been restricting biometric collection by schools and government actors for years.[50] Existing and pending state biometric privacy laws tend to fall into three categories: laws that restrict the collection of

---

[43] *Id*.

[44] Glaser, *supra* note 5.

[45] *See generally* Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, AM. BAR ASS'N (May 2016), https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html (recognizing that the popularity and privacy concerns associated with biometric technology have caused states to regulate collection of biometrics).

[46] 740 ILL. COMP. STAT. 14/20 (2008).

[47] 11 TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009).

[48] H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017); *Washington Becomes Third State to Enact Biometric Privacy Law*, HUNTON & WILLIAMS PRIVACY & INFO. SEC. BLOG (June 1, 2017), https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/.

[49] Grossenbacher & Kelleher, *supra* note 21.

[50] Claypoole & Stoll, *supra* note 45.

biometrics belonging to students, laws that restrict the collection of biometric information by government entities, and laws that restrict the collection of biometric information by businesses.[51] Despite its commercial nature, the healthcare industry is exempted by state biometrics laws because medical privacy is protected by the federal Health Insurance Portability and Accountability Act (HIPAA).[52] Many states, including North Carolina and West Virginia, already protect the biometric information of students at K-12 schools.[53] These states restrict the collection of student biometric information by only allowing disclosure with parental consent and requiring the information to be destroyed once the owner of the biometric data graduates or switches schools.[54] Maine and New Hampshire restrict the collection of biometric data related to personal identification, like driver's licenses, but they allow biometric data collection for law enforcement or immigration purposes.[55] Even though many states protect citizens against specific instances of biometric collection, only Illinois, Washington, and Texas have laws that prevent the collection of biometrics for general commercial use.[56]

A. *The Illinois Biometric Information Privacy Act*

Illinois became the first state to regulate the commercial gathering of biometric information by enacting the Biometric Information Privacy Act (BIPA) in 2008.[57] "Biometric information," as broadly defined by the Act, means "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual;" it further defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[58] BIPA

---

[51] *Id*.

[52] 740 ILL. COMP. STAT. 14/10 (2008).

[53] N.C. GEN. STAT. § 115C‑402.5 (2016); W. VA. CODE § 18-2-5h (2012).

[54] N.C. GEN. STAT. § 115C‑402.5; W. VA. CODE § 18-2-5h; *see also* Claypoole & Stoll, *supra* note 45.

[55] ME. STAT. tit. 29, § 1401 (2009); N.H. REV. STAT. ANN. § 260:10-b (2014).

[56] COMP. STAT. 14/10; 11 TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009); H.B. 1493, 65 Leg., Reg. Sess. (Wash. 2017); 2017 Wash. Sess. Laws 1141.

[57] COMP. STAT. 14/10.

[58] *Id*.

prohibits selling, trading, leasing or otherwise profiting from collected biometric data and mandates transparency in the collection, use, and storage of that data.[59] In addition, the Act requires corporations to obtain written consent from employees and customers when acquiring, using, or storing biometric information from these individuals.[60] The Act provides consumers and employees a private right of action for violations.[61] Photographs, digital signatures, writing samples, and biological samples are excluded from coverage under BIPA.[62]

Since its passage, BIPA has been a lightning rod for legal action.[63] Between July 2017 and publication, twenty-six class-action lawsuits have been filed against Illinois employers under BIPA.[64] Most of the employee-filed lawsuits assert that employers, including Speedway and InterContinental Hotels Group, are collecting and storing fingerprint data without consent.[65] The plaintiffs in those suits are accusing the employers of collecting the fingerprints from machines that use biometric data to clock in employees for their shifts.[66] By not obtaining consent or notifying employees of how their biometric information is being collected and stored, employers violate BIPA.

The flood of BIPA lawsuits is not limited to employees suing employers; consumers are also turning to BIPA to protect their biometric information in both state and federal court.[67] One notable

---

[59] *Id*.

[60] *Id.*; *see also* Amy Korte, *Illinois Employers Flooded with Class-Action Lawsuits Stemming from Biometric Privacy Law*, ILL. POL'Y (Oct. 17, 2017), https://www.illinoispolicy.org/illinois-employers-flooded-with-class-action-lawsuits-stemming-from-biometric-privacy-law/.

[61] COMP. STAT. 14/10.

[62] *Id*.

[63] Korte, *supra* note 60 (establishing that Illinois has seen a massive number of lawsuits under BIPA since it was passed in 2008).

[64] *Id*.

[65] Complaint, Howe v. Speedway, LLC, No. 1:17-CV-07303 (N.D. Ill. filed Oct. 10, 2017); Complaint, Zepeda v. InterContinental Hotels Group, No. 2017-CH-08904 (Ill. Cir. Ct. filed June 27, 2017); *see also* Korte, *supra* note 60.

[66] Korte, *supra* note 60.

[67] *See* Justin Lee, *Facebook Facial Recognition Lawsuit Put on Hold*, BIOMETRIC UPDATE (Feb. 9, 2017), http://www.biometricupdate.com/201702/facebook-facial-recognition-lawsuit-put-on-hold; *see also Facing Privacy Suits*

federal BIPA case revolves around Facebook's facial recognition software.[68] The plaintiffs could file in federal court because they were diverse parties pursuant to 28 U.S.C. § 1332.[69] The plaintiffs in the lawsuit against Facebook claimed that the website's tag suggestion feature violates BIPA by collecting and storing unique biometrics identifiers data from their uploaded images without providing written notice or gaining consent from their users.[70]

The social media giant defended its activity by asserting the plaintiffs must prove an injury in fact resulting from the site's misuse of biometric information, not just a technical violation of BIPA, to maintain standing.[71] An injury in fact must be "an invasion of a legally protected interest" that is "concrete and particularized" and cannot be "conjectural or hypothetical."[72] On top of its assertion that the plaintiffs do not have standing, Facebook also contends that BIPA violates the Commerce Clause[73] and that the site's users actually do consent to the usage of facial recognition software when they allow themselves to be tagged in online photos.[74]

About Facial Recognition: BIPA Cases Move Forward as More States Consider Passing Biometric Data Laws, HUNTON & WILLIAMS PRIVACY & INFO. SEC. BLOG (Oct. 4, 2017), https://www.huntonprivacyblog.com/2017/10/04/facing-privacy-suits-about-facial-recognition-bipa-cases-move-forward-as-more-states-consider-passing-biometric-data-laws/.

[68] *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2017) (holding that the plaintiff users stated a claim under BIPA).

[69] *See* 28 U.S.C. § 1332 (2012) (stating that federal courts have subject matter jurisdiction over diversity cases where the parties are citizens of different states and the amount in controversy exceeds $75,000).

[70] *See In re Facebook Biometric Info*. *Privacy Litig*., 185 F. Supp. 3d at 1172.

[71] *Id*.

[72] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (quoting Lujan v. Defs. of Wildlife, 112 S. Ct. 2130, 2134 (1992)).

[73] *See* Justin Lee, *Facebook Says Illinois Biometrics Privacy Law Violates Constitution*, BIOMETIRC UPDATE (Nov. 21, 2016), http://www.biometricupdate.com /201611/facebook-says-illinois-biometrics-privacy-law-violates-constitution (claiming that the BIPA violated the Commerce Clause of the U.S. Constitution because it allows Illinois to improperly strain or discriminate against interstate commerce).

[74] Jared Bennett, *Facebook: Your Face Belongs to* Us, THE DAILY BEAST (July 31, 2017), https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition.

B. *BIPA Litigation & Standing Requirements*

The federal suit against Facebook has reached the Ninth Circuit, but the Court has delayed issuing a ruling, pending the outcome of the recently remanded *Spokeo* case.[75] The issue in *Spokeo* was whether a per se violation of the Fair Credit Reporting Act (FCRA) constituted an injury in fact in the context of a federal standing inquiry.[76] In August 2017, the Ninth Circuit held that a per se violation of FCRA was enough to trigger a private cause of action under the act even if the plaintiffs did not suffer concrete injuries.[77] The per se violation in *Spokeo* was the misrepresentation of the plaintiff's employment status, age, and marital status.[78] More specifically, the Ninth Circuit stated that "intangible harms" can constitute an injury in fact when the violation of a federal statute presents "a risk of real harm" to a "concrete interest."[79] Essentially, the Ninth Circuit's most recent *Spokeo* decision determined that per se violations of a statute, like misrepresenting a user's personal information, will satisfy the injury in fact component of a standing analysis only if there is a risk of actual monetary or physical harm.

A Ninth Circuit decision on the BIPA lawsuit against Facebook is likely to be issued soon since *Spokeo* has been decided on remand. Based on the Ninth Circuit's more recent holding in *Spokeo*, the plaintiff's suing Facebook have a strong argument in favor of proper standing if they can establish a per se BIPA violation and can also prove that the violation could cause "concrete harm."[80] Considering that stolen biometric identifiers can be used to access the victim's bank information,[81] per se BIPA violations could easily result in concrete harms. Since the Ninth Circuit's newly released *Spokeo* decision concerned a federal rather than state law, the court will

---

[75] Spokeo, Inc. v. Robins, 136 S. Ct. at 1548.

[76] *Id*.

[77] Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017), *cert. denied* 138 S.Ct. 931.

[78] *Id*. at 1115.

[79] *Id*. at 1113.

[80] *Id*. at 1108.

[81] Michael Corkery, *Goodbye, Password. Banks Opt to Scan Fingers and Faces Instead.*, N.Y. TIMES (June 21, 2016), https://www.nytimes.com/2016/06/22/business/dealbook/goodbye-password-banks-opt-to-scan-fingers-and-faces-instead.html.

have to decide if the holding will apply to the Facebook case.[82] If *Spokeo* is applied to state laws like BIPA, the plaintiffs have a strong argument that a per se violation will qualify as an injury in fact.

Defendants fighting BIPA lawsuits in state court have also raised plaintiff's lack of standing as an argument to dismiss.[83] An Illinois appellate court addressed the standing issue stemming from BIPA in *Rosenbach v. Six Flags Entertainment Corp*.[84] The plaintiff in *Rosenbach* was a mother who purchased a season pass to Six Flags theme park for her minor son.[85] Six Flags obtained the son's fingerprint for biometric identification so he could be associated with the season pass his mother purchased.[86] The plaintiff asserted Six Flags did not provide her or her son with written consent forms and that she did not consent to the use of a scanner to collect her son's fingerprints when he obtained the pass.[87] She did not claim that any physical or monetary harm resulted from the fingerprint scanning, but she did identify per se violations of BIPA, which prompted Six Flags to question whether the plaintiff was an "aggrieved" party under BIPA.[88] *Rosenbach* argued that a privacy violation codified by BIPA is enough of an injury to warrant punishment under the act.[89] The statute does not define aggrieved, so the Second District Appellate Court of Illinois construed the term to mean some "adverse effect or harm resulting from the violation."[90]

---

[82] Robins v, Spokeo, Inc., 867 F.3d at 1113.

[83] *See* Paul Tassin, *Six Flags Biometric Privacy Class Action Must Allege Actual Harm, Says Court*, TOP CLASS ACTIONS (Dec. 27, 2017), https://topclassactions.com/lawsuit-settlements/lawsuit-news/829665-six-flags-biometric-privacy-class-action-must-allege-actual-harm-says-court/ (explaining that plaintiffs suing under BIPA in Illinois state court do not have standing unless there has been an injury in fact).

[84] Rosenbach v. Six Flags Entm't Corp., 2017 Ill. App. 160317; *see* Tassin, *supra* note 83.

[85] *Rosenbach*, 2017 Ill. App. 2d 160317 at ¶ 7–10; *see* Tassin, *supra* note 83.

[86] *Rosenbach* at ¶ 7–10.

[87] *Id*.

[88] *Id*.; *see* Tassin, *supra* note 83.

[89] *See* Tassin, *supra* note 83.

[90] *Rosenbach*, 2017 Ill. App. 2d 160317 at ¶ 20.

The Illinois appellate court's interpretation means that state lawsuits under BIPA will require more than a technical violation, such as not notifying consumers of the finger scanning process.[91] Based on the holding in *Rosenbach*, citizens interested in filing a BIPA lawsuit in state court will likely have to prove that a violation caused them to experience tangible, concrete harm. *Rosenbach*'s holding conflicts with the Ninth Circuit's recent *Spokeo* decision because it bars plaintiffs filing in state court from establishing an injury in fact based on the possibility of tangible harm, while *Spokeo* would allow this in federal court.[92] This tension forces plaintiffs to either establish tangible harm, such as a compromised bank account, or attempt to file a diversity action in federal court.[93] BIPA is a step forward in protecting the biometric information of Illinois's citizens, but standing conflicts could chill private suits seeking to enforce the act.

C. *Texas & Washington's Biometric Privacy Laws*

Texas passed the nation's second commercial biometric privacy law, the Texas Biometric Privacy Act (BPA), in 2009.[94] Like the Illinois BIPA, the Texas BPA aims to restrict and regulate the commercial collection, retention, and disclosure of biometric identifiers.[95] However, the BPA does not offer Texans a private right of action, leaving the attorney general as the law's only enforcer.[96] In the Texas statute, "biometric identifiers" are defined as "retina or iris scans, fingerprints, voiceprint, or the recording of hand or face geometry."[97] The definition of biometric identifiers in the Texas

---

[91] *See* Tassin, *supra* note 83.

[92] Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (9th Cir. 2017), *cert. denied* 138 S.Ct. 931.

[93] 28 U.S.C. § 1332 (2012).

[94] 11 TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009); Annemaria Duran, *Understanding the Texas Biometric Privacy Law as an Employer*, SWIPECLOCK WORKFORCE MGMT. (Dec. 29, 2017), https://www3.swipeclock.com /understanding-texas-biometric-privacy-law-employer/.

[95] BUS. & COM. § 503.001.

[96] *Id*.; *see* Tumeh, *supra* note 27 (explaining Texas wanted a more business-friendly biometrics law so they could strike a better balance between privacy and corporate interests than Illinois).

[97] BUS. & COM. § 503.001.

statute closely mirrors that of the Illinois statute. Unlike Illinois, the Texas BPA only requires notice, not written consent, for the collection of biometric identifiers.[98] Both statutes require the destruction of stored biometric identifiers once certain requirements are met.[99] Yet another difference between the Illinois law and the Texas law is that the former completely bans the sale and leasing of commercially obtained biometric identifiers while the latter allows for sale and leasing if a narrow set of conditions are met.[100] In Texas, businesses can sell or lease biometric information acquired from customers or employees if the information is necessary to complete a financial transaction expressly authorized by the individual that provided the data.[101]

While the Illinois BIPA and the Texas BPA both restrict the commercial collection, storage, and disclosure of biometric information, the lack of a written consent requirement, the inability for citizens to file suits, and the ability to sell or lease biometrics make Texas's law more favorable to businesses than Illinois's.[102] Allowing businesses to disclose biometric identifiers for a specific purpose, like the completion of a transaction on behalf of the client who submitted the information, is a reasonable concession to businesses.[103] In contrast, excluding a private right of action for citizen enforcement and requiring notice, not consent, for the collection of biometric identifiers means the law does not go far enough to protect consumer privacy.[104] State legislatures need to balance competing privacy and business interests when drafting biometric privacy statutes; instead, Texas's legislature drafted an imbalanced law that favors businesses.[105]

---

[98] *Id*.; Tumeh, *supra* note 27.

[99] *See* Tumeh, *supra* note 27 (noting that the Illinois law requires destruction after the purpose of the information has been satisfied or three years after the individual's last contact with the corporation and that Texas law requires destruction within a reasonable amount of time, up to a maximum of one year, from when the purpose of the biometric information expires).

[100] BUS. & COM. § 503.001; Tumeh, *supra* note 27.

[101] BUS. & COM. § 503.001.

[102] 740 ILL. COMP. STAT. 14/20 (2008); BUS. & COM. § 503.001.

[103] BUS. & COM. § 503.001.

[104] *Id*.

[105] Tumeh, *supra* note 27.

Washington's new biometric privacy act is more similar to Texas's somewhat lenient BPA than to Illinois's strict BIPA. The Washington Act is favorable to businesses, but it still differs from its counterparts in a number of ways.[106] First, the law's definition of "biometric identifiers" includes data or measurements from irises, fingerprints, retinas, voices, and "other unique biological characteristics or patterns," but it does not list facial geometry.[107] In comparison, both Texas and Illinois include facial geometry in their definitions of "biometric identifiers."[108] Second, the language of the Washington statute forbids a person from "enroll[ing] a biometric identifier for a commercial purpose without first providing notice, obtaining consent or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[109] "Person" means an "individual, partnership, corporation, limited liability company, organization, association, or any other legal or commercial entity" as defined by the statute.[110] Additionally, "enroll" 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."[111] The Washington BPA does not define "mechanism," and no cases have been filed requiring the term to be interpreted leaving businesses with no guidelines to follow when implementing a biometric privacy program.[112]

Washington's law differs from Illinois's and Texas's in not only its language but also in offering businesses more methods of complying with the law.[113] Other characteristics of the Washington

---

[106] COMP. STAT. 14/20; BUS. & COM. § 503.001; H.B. 1493, 65th Leg. Reg., Reg. Sess. (Wash. 2017).

[107] H.B. 1493.

[108] COMP. STAT. 14/20; BUS. & COM. § 503.001; *see also* Tumeh, *supra* note 27.

[109] H.B. 1493.

[110] *Id*.

[111] *Id*.

[112] *Id*.

[113] *See id*. (offering businesses the ability to comply with the law's notification requirements by asking for consent or even just making customers and employees

law that mirror the Texas law are the absence of a private right of action and the ability of businesses to sell, lease, and disclose biometric information under certain circumstances.[114] In fact, the Washington law is less restrictive of disclosure than the Texas law because the former carves out more exceptions that allow businesses to share biometric identifiers with other businesses.[115] Privacy advocates argue that although the Washington law and the Texas BPA improve biometric security, they both "lack teeth" because citizens cannot enforce either one by bringing suits for violations.[116] Without a private right of action, government attorneys decide when to punish businesses for biometric privacy violations.[117] Since the attorneys enforcing the Washington statute and the Texas BPA will have discretion over what cases to pursue, citizens with valid claims may be ignored.[118] Since citizens do not have a private right of action under the Texas and Washington laws, neither state has experienced the flood of biometric privacy litigation that Illinois has.[119]

D. *Why Haven't More States Passed Commercial Biometric Privacy Laws?*

As of January of 2018, Illinois, Washington, and Texas are still the only three states that have enacted commercial biometric privacy laws.[120] Three interconnected concerns are holding back other states from passing similar laws: the potential for class-action lawsuits, the exact wording of state biometric laws, and individual state interests

---

aware of what companies use the biometric information for); HUNTON & WILLIAMS PRIVACY & INFO. SEC. BLOG, *supra* note 48.

[114] *See* Tumeh, *supra* note 27 (listing circumstances that allow Washington businesses to sell, lease, and disclose biometric information).

[115] H.B. 1493; Tumeh, *supra* note 27.

[116] Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG BNA (July 18, 2017), https://www.bna.com/washington-biometric-privacy-n73014461920/.

[117] *Id*.

[118] *Id*.

[119] *Id*.

[120] Hanley Chew & Eric Ball, *The Impact of the Surge of Biometric Data Privacy Lawsuits Against Employers*, L.J. NEWSL. (Jan. 2018), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2018/01/01/the-impact-of-the-surge-of-biometric-data-privacy-lawsuits-against-employers/.

in business development.[121] Despite its enactment in 2008, the Illinois BIPA has only recently become the centerpiece of numerous lawsuits against major tech companies including Facebook,[122] Google,[123] and Shutterfly.[124] Legislators in other states likely do not want to open the floodgates to a wave of class-action lawsuits by passing a biometric privacy law too similar to the Illinois BIPA.[125] In response to the barrage of BIPA lawsuits in Illinois, others states "may either reconsider the scope of their proposed biometric data privacy laws or the wisdom of even enacting such laws."[126]

If other states are committed to passing their own commercial biometric privacy laws, they will have to decide how broad such a law should be. The Illinois BIPA was once seen as a "possible model" for similar laws, but class-action lawsuits and aggressive lobbying from companies interested in collecting biometric information, such as Facebook and Google, have scared states away from strict limits on the usage of biometric information and the inclusion of a private right of action.[127] Without a viable model over which technology companies and privacy advocates can compromise, state legislatures have struggled to pass new biometric privacy laws.[128] Seven states have laws currently pending, but cannot get the votes to finally pass them.[129] Legislators in New York struggled to even complete a proposal because of debate over how to define "biometrics."[130] The Washington biometric privacy act, which does not yet have an official title and was passed just last year,

---

[121] *Id*.

[122] *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2017).

[123] Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

[124] Norberg v. Shutterfly, 152 F. Supp. 3d 1103 (N.D. Ill. 2015).

[125] *See* Chew & Ball, *supra* note 120.

[126] *Id*.

[127] Kartikay Mehrotra, *Tech Companies Are Pushing Back Against Biometric Privacy Laws*, BLOOMBERG BUSINESSWEEK (July 19, 2017 8:26 PM), https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws.

[128] *Id*.

[129] Chew & Ball, *supra* note 120.

[130] Assemb. A9793, 241st Leg. Sess., Reg. Sess. (N.Y. 2018); Mehrotra, *supra* note 127.

is one of the "best example[s] of industry pushback on attempts to regulate biometric data" because of its business-friendly biometric collection requirements and its lack of a citizen suit provision.[131] One of the bill's co-sponsors, Washington Representative Mark Harmsworth, revealed that if the bill included a private right of action, he was unsure it would have passed.[132] Consumer rights organizations arguing for strict biometric privacy laws and tech giants lobbying for business-friendly provisions, or even against the passage of such laws as a whole, has made drafting, much less passing, biometric privacy laws almost impossible.

Instead of "reconsidering the scope" of potential biometric privacy laws, some states may not even attempt to pass them.[133] Biometric privacy laws may deter businesses from expanding to states that have enacted these types of statutes,[134] and some states may not be willing to sacrifice that growth in exchange for enhanced consumer privacy. States considering biometric privacy laws must also consider how such a law would affect businesses already in operation, particularly corporations that have an interest in utilizing their customers' biometric identifiers. Potential liability under a new biometric privacy law could force corporations to stop working on innovative projects, or even leave the state entirely.[135] Jeff Morris, the other co-sponsor of Washington's biometric privacy act, said that balancing privacy rights and technological innovation "was a challenge." A federal biometric privacy law would alleviate the pressure on states to balance economic development, innovation, and consumer privacy. Simply put, zealous lobbying on behalf of technology companies, lack of a model statute that privacy and technology proponents can agree on, and fear of opening the door to more class-action lawsuits have stopped other states from successfully passing biometrics privacy laws.

---

[131] H.R. 1493, 65th Leg., Reg. Sess. (Wash. 2017); Mehrotra, *supra* note 127.
[132] Shukovsky, *supra* note 116.
[133] Chew & Ball, *supra* note 120.
[134] *See id.*
[135] *See id.*

E. *A Survey of American Privacy Law*

Passing a federal law can be an arduous process.[136] Until a federal law focused solely on biometric privacy is passed, the states, and to a lesser extent, existing federal laws, will bear the primary burden of protecting citizens' biometric information.[137] To avoid a drawn-out federal legislative process that still may not produce a law, Congress may be able to add biometric privacy provisions, like the ones already in the HIPAA and the Gramm-Leach-Bliley Act (GLBA).[138] After all, the United States has been fighting to protect the privacy of its citizens since its humble beginnings.[139] Samuel D. Warren and Louis Brandeis catapulted privacy law into mainstream prominence when the Harvard Law Review published their article *The Right to Privacy* in 1890.[140] Warren and Brandeis' article discusses an inherent right to privacy, the interplay between that right, tort law, and intellectual property law, and both authors' perceived limits on the right.[141] *The Right to Privacy* garnered widespread attention[142] and paved the way for the privacy revolution that took place after the turn of the century.[143]

---

[136] *See* Elahe Izadi & Clare Foran, *Why Congress Sometimes Can't Even Pass Moderate, Bipartisan Bills*, THE ATLANTIC (Sept. 15, 2013), https://www.theatlantic.com/politics/archive/2013/09/why-congress-sometimes-cant-even-pass-moderate-bipartisan-bills/444849/ (addressing the difficulty of passing federal laws even when they are "watered down" and receive bipartisan support).

[137] *See* Claypoole & Stoll, *supra* note 45.

[138] *See* Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320 (2012); Graham-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

[139] *See generally* Daniel J. Solove, *A Brief History of Information Privacy Law in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 1:2 (Kristen Mathews ed., 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271 (analyzing the earliest American safeguards against privacy violations including the Third, Fourth, and Fifth Amendments).

[140] Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[141] *See id.*

[142] *See* Fred R. Shapiro & Michelle Pearse, *The Most-Cited Law Review Articles of All Time*, 110 MICH. L. REV. 1483, 1489 (2012) (citing *The Right to Privacy* as the second most-cited law review article of all time).

[143] *See* Solove, *supra* note 139.

At the beginning of the 1900s, existing laws in the United States were insufficient to handle the growing privacy concerns stemming from evolving technology and citizens started filing "privacy tort" lawsuits to protect their rights.[144] In response to growing concerns about wiretapping and the Supreme Court's 5-4 decision in *Olmstead v. United States*,[145] the federal government began to pass privacy laws to protect its citizens starting with the Federal Communications Act of 1934.[146] The remainder of the 20th century saw the narrowing of the Fourth Amendment, although during that same time period Congress passed numerous federal privacy laws to protect Americans against government and corporate intrusion.[147] One of the privacy laws, and the first health privacy law, passed during the 20th century was HIPAA.[148]

HIPAA was passed in 1996 as a part of a congressional push for healthcare reform in response to growing national concern over the privacy of confidential information disclosed to healthcare providers and insurance companies.[149] Amongst other mandates that are not relevant to this Recent Development, HIPAA ensures that personal information Americans provide to healthcare providers remains confidential.[150] Furthermore, HIPAA "mandates uniform standards for electronic data transmission of administrative and financial data relating to patient health information."[151] Violations of HIPAA can be costly; multiple violations in a single calendar year

---

[144] *See id*. (explaining that new technology, like photography, led to privacy torts, such as intrusion upon seclusion and public disclosure of private facts, against media outlets).

[145] 277 U.S. 438 (1928) (holding that wiretaps were not unreasonable searches and seizures under the Fourth Amendment).

[146] Solove, *supra* note 139.

[147] *Id*. (listing laws passed that protect the privacy of Americans and chronicling cases that condensed the scope of the Fourth Amendment to not protect against activities like pen register identification).

[148] *Id*.

[149] *HIPPA Background*, U. OF CHI. MED. CTR, http://hipaa.bsd.uchicago.edu/background.html, (last updated Feb. 2010).

[150] *Id*. (identifying the different types of information covered by HIPAA which includes patient names, medical records, phone numbers, social security numbers, and even biometric information such as finger and voice prints).

[151] *Id*.

will result in fines in excess of $1,000,000.[152] HIPAA was installed after the public pushed for healthcare reform, but HIPAA only protects biometric privacy in one industry. Further, citizens alleging HIPAA violations actually have no private federal right of action; they can only file complaints to be investigated by the Department of Justice or a state Attorney General's office.[153] If the Department Justice or an Attorney General decides that a HIPAA claim has merit, a case will be filed.[154] The lack of a citizen suit provision may mean that legitimate claims could get ignored by the Department of Justice or an Attorney General's office if they decide a case is not worth filing. Certain existing federal laws include biometric privacy provisions, but these laws are insufficient because they do not provide uniform protection for all Americans against all industries.[155]

F. *Which Existing Federal Laws Address Biometric Privacy?*

HIPAA is just one example of the many federal privacy laws promulgated by Congress during the 20th century.[156] Federal law takes a "sectoral approach" to privacy, meaning that "the primary source of privacy laws in the United States takes the form of various laws governing industry sectors."[157] HIPAA, GLBA, and the Family Educational Rights and Privacy Act (FERPA) all have provisions that include biometric privacy.[158] HIPAA lists various categories of "protected health information" (PHI) that are subject to data transfer restrictions. Financial institutions must comply with the GLBA which mandates the protection of "non-public personal

---

[152] *Id*.

[153] Kane Russell Coleman Logan, PC, *Is There a Private Cause of Action for HIPAA Violations?*, LEXOLOGY (Jan. 28, 2016), https://www.lexology.com/library/detail.aspx?g=a5bc1a0f-557a-4bf1-8cd3-1498c872a4dc.

[154] *Id*.

[155] *Id*.

[156] The Privacy Act of 1974, 5 U.S.C. § 552a, and the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.), are two of the other federal privacy laws passed in the 20th century.

[157] Claypoole & Stoll, *supra* note 45.

[158] *Id.*

information."[159] Although biometric identifiers are not explicitly mentioned in GLBA, non-public personal information is read broadly to include things that would be considered biometric identifiers.[160] Unfortunately, the GLBA allows for the sale of non-public information and is silent on consent for the acquisition of that same information, giving rise to the question of whether or not the law actually safeguards biometric privacy.[161] This question is further complicated by the dual status of biometric information, discussed in Part I. Although biometric identifiers are unique to individuals, making them private, the whole world can see, and possibly duplicate, those identifiers, making them public as well. For GLBA to apply to biometric information, lawyers will need to navigate this odd dichotomy. Lastly, educational institutions are explicitly restricted from disclosing student biometric information without parental consent under FERPA.[162] Some exceptions to FERPA apply, but its provisions provide far more robust safeguards than the GLBA.[163]

G. *Which Existing State Laws Address Biometric Privacy?*

Many states that have not passed or introduced a biometric privacy bill have addressed the topic in existing laws.[164] For example, North Carolina used an existing law, the Identity Theft Protection Act, to protect biometric privacy because it included "biometric data" as a form of identifying information.[165] The North Carolina law "requires any entity conducting business in the state and maintaining personal information of a resident to take reasonable measures to protect the information against unauthorized access."[166] Many other states also have data breach laws that protect biometric information, including South Carolina.[167] The South

---

[159] *Id*.; Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

[160] Claypoole & Stoll, *supra* note 45.

[161] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338.

[162] Family Educational Rights & Privacy Act, 20 U.S.C. § 1232g (2012).

[163] *Id*.

[164] Claypoole & Stoll, *supra* note 45.

[165] N.C. GEN. STAT. § 75-60 to 66 (2005).

[166] Claypoole & Stoll, *supra* note 45; *accord* N.C. GEN. STAT. § 75-64(a).

[167] S.C. CODE ANN. § 37-20-110 (2008).

Carolina law includes "information issued by a governmental or regulatory entity that will uniquely identify an individual" in its definition of "personal identifying information."[168] This broad definition could be construed to include information like fingerprints or retina data, but since it does not explicitly list biometric information within its definition of "personal identifying information," protection is not guaranteed.

H. *Why State Laws and Existing Federal Laws Do Not Adequately Protect Biometric Privacy*

Existing state and federal laws do not adequately protect biometric privacy in the United States. The sectoral approach to privacy regulation is simultaneously too restrictive and not restrictive enough.[169] Many federal privacy laws overlap with one another because many businesses walk a thin line between one or more sectors leading to excess regulation.[170] The unfortunate businesses subject to multiple privacy laws struggle to comply with the seemingly endless number of uncertain, inconsistent provisions.[171] On the opposite end of the privacy regulation spectrum sit businesses and organizations that fall into the many gaps created by dividing our economy into sectors. Passing a federal biometric privacy law would set uniform standards for commercial organizations across the country, and even though the standards may require some interpretation, it would eliminate sectoral gaps. The argument against letting the states serve as the primary defenders of biometric privacy is far less complex: state laws only extend so far. A federal law will provide protection for the biometric information of every American and states will not need to pass their own laws or scramble to adapt existing laws to the new concerns surrounding biometrics.

---

[168] *Id.*; Claypoole & Stoll, *supra* note 45.
[169] Solove, *supra* note 139.
[170] *Id*.
[171] *Id*.

IV. WHAT SHOULD A FEDERAL BIOMETRIC PRIVACY LAW LOOK LIKE?

Despite the array of federal privacy laws that Congress has signed into law, no reports had surfaced at the time of this Recent Development identifying legislation that addresses commercial biometric privacy. If legislation is introduced, Congress will have to decide how to define the term "biometric identifier," what limits to set on the collection and storage of biometric information, whether or not businesses should be able to sell, or disclose that same information, and finally whether or not to include a private right of action.[172] Making decisions on the exact wording of a federal biometrics law will be complicated by the immense lobbying power large technology companies wield.[173] Corporate lobbying efforts resulted in the watered-down biometric privacy law that Washington passed and have even stopped other states from passing similar laws entirely.[174] If Congress decides to introduce a biometric privacy bill, it must properly balance consumer rights and business development in a way that makes the bill politically viable.

A. *How a Federal Law Should Define "Biometric Identifiers"*

Congress could use a definition similar to those contained in Texas and Illinois statutes, or they could use a less detailed, but potentially broader, definition like Washington's.[175] Alternatively, Congress could use the Biometric Research Group's expansive definition of biometrics, which includes both physical and behavioral characteristics.[176] To be as inclusive as possible, Congress could even use the Biometric Research Group's definition and then add a non-exhaustive list of biometric identifiers for

---

[172] *See* Tumeh, *supra* note 27.

[173] *See* Brian Fung & Hamza Shaban, *To Understand How Dominant Tech Companies Are, See What They Lobby For*, L.A. TIMES (Sept. 1, 2017, 12:55 PM), http://www.latimes.com/business/technology/la-fi-tn-silicon-valley-lobbying-20170901-story.html (describing the impact that technology companies have on national politics, particularly legislation).

[174] H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017); Chew & Ball, *supra* note 120.

[175] Wash. H.B. 1493.

[176] Tumeh, *supra* note 27.

clarity.[177] A federal biometric privacy law should be expansive and forward-thinking, meaning that Congress should embrace the Biometric Research Group's definition and formulate their own non-exhaustive list of identifiers. This would expand the law to cover not only physical characteristics but also behavioral characteristics.[178] Adding a non-exhaustive list of biometric identifiers to the definition of biometrics would make the law adaptable enough to sufficiently cover both existing, and future, applications of biometric identification technology. Litigation deciding whether certain characteristics should be considered a biometric identifier is inevitable, so Congress should list as many identifiers as they can to at least reduce the number of lawsuits. The constantly evolving field of biometrics precludes Congress from developing a complete list of biometric identifiers, but that should not stop them from drafting the most inclusive definition possible. While predicting future applications of biometric technology is difficult, a clause preceding the non-exhaustive list of identifiers that clearly states the list is subject to expansion is necessary.

B. *How a Federal Law Should Address the Collection and Storage of Biometric Information*

First and foremost, Congress must decide if a federal law should require notice and consent for the collection of biometric information, like Illinois, or just notice, like Texas and Washington.[179] To make the federal law's collection section even more robust, Congress could even require a unique document for biometric collection completely separate from any user agreements or other corporate documents. By creating a unique consent form for the collection of biometric information, citizens would be less likely to blindly sign away their biometric identifiers as part of a massive user agreement. Including notice and consent requirements would hold commercial entities to a higher standard and is thus the preferable approach for Congress to take.

---

[177] King, *supra* note 2.

[178] *Id*.

[179] 740 ILL. COMP. STAT. 14/20 (2008); 11 TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009); Wash. H.B. 1493.

After determining how to restrict the collection of biometric information, Congress will then need to lay out requirements for the safe storage and timely destruction of biometric records. The least restrictive storage requirement Congress could mandate is one that allows commercial entities to maintain biometric records for "a reasonable time."[180] Washington's biometric privacy uses this broad storage provision, and because the law is so new, the outer limits of the standard have not been established.[181] Washington also supplements its "reasonable time" storage mandate with three exceptions that allow businesses to store the information longer.[182] Texas and Illinois included similar "reasonable time" requirements and added time limits on storage as well.[183] To strike the proper balance between privacy rights and business interests, Congress should model federal storage and destruction provisions after the ones employed by Texas and Illinois. A maximum storage period set three years, or less, from the collection of the information could be combined with carveouts for businesses that have exceptional reasons to maintain biometric records for longer and a "reasonable time" standard to produce the best storage and mandatory destruction provision possible.

C. *Proposed Characteristics of a Provision on the Sale and Disclosure of Biometric Information*

The third significant consideration Congress will need to address is the sale and disclosure of biometric information.[184] Illinois completely banned the sale of biometric information but allows for

---

[180] Tumeh, *supra* note 27.

[181] Wash. H.B. 1493.

[182] *Id.* (establishing that information can be stored for longer than reasonably necessary if: it is necessary to comply with a court order; protect the business against fraud, criminal activity, claims, security threats, or liability; or provide services for the purpose the information was enrolled).

[183] COMP. STAT. 14/20; BUS. & COM. § 503.001 (explaining that Texas imposed a one-year time limit on biometric retention unless an enumerated exception applies and that Illinois imposed a three-year time limit on biometric retention from the last interaction the source of the information had with the company in question).

[184] Tumeh, *supra* note 27.

disclosure if required by another law.[185] BIPA also allows disclosure if a company is faced with a subpoena, warrant, or if disclosure is "necessary to complete a financial transaction."[186] For disclosure to be authorized under any scenario, BIPA requires consent from the individual that provided the biometric information.[187] Washington and Texas let commercial entities sell and disclose biometric information if certain exceptions apply.[188] Texas's list of exceptions for disclosure is the same as Illinois's list, and the former applies those same exceptions to the sale of biometric information.[189] Washington's list of exceptions for the sale and disclosure of biometric information includes the ones listed by Texas and Illinois in addition to four more exceptions.[190] To strike a balance between corporate interests and biometric privacy, Congress should adopt the Texas approach. Giving businesses the right to sell and disclose biometric information in a small number of circumstances will protect privacy interests and will not stifle a business's ability to operate.

D. *Should a Federal Law Include a Private Right of Action? Absolutely.*

The final major decision that Congress will need to make is whether to include a private right of action such as the one in Illinois's BIPA.[191] Adding a private right of action will give the law the "teeth" that detractors of Texas and Washington's laws are clamoring for, but it could also raise a number of legal questions and lead to a flood of new lawsuits.[192] Meticulous drafting will not save

---

[185] COMP. STAT. 14/20.

[186] *Id*.

[187] *Id*.

[188] BUS. & COM. § 503.001; H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017).

[189] COMP. STAT. 14/20; BUS. & COM. § 503.001; *see also* Tumeh, *supra* note 27.

[190] Wash. H.B. 1493 (listing compliance with the statute's notice, consent, security, and retention requirements, necessity to provide a service to the person that provided the information, a contractual promise not to engage in future disclosure, and preparation for litigation as four additional situations that allow for disclosure).

[191] COMP. STAT. 14/20.

[192] Shukovsky, *supra* note 116.

an extremely innovative federal law governing biometric privacy law from lawsuits hinging on statutory interpretation. That being said, clearly defining relevant terms and producing a comprehensive law will minimize litigation. Moreover, a private right of action will give consumers and employees the power to protect their rights without relying on an Attorney General's office. Other laws, like HIPAA, have only proven that submitting claims to a government office for review will not always provide the same level of protection as a citizen suit provision.[193] Government attorneys have limited time and resources to investigate claims so every violation submitted will not be given equal consideration. Compromised biometric databases could ruin the lives of countless Americans, and cases involving delicate biometric information should not be selectively pursued based on the discretion of a small group of attorneys. An increase in litigation stemming from a citizen suit provision is a small price to pay for more robust protection of American biometric information. Congress needs to balance privacy and business interests to make sure a federal biometric privacy law is politically viable, but they cannot fold under pressure from the tech sector and exclude a private right of action from the statute.

V. CONCLUSION

The explosion of interest in biometrics across the United States over the last few years has raised serious concerns about the safety of biometric technology and what businesses do with biometric information. The utility of biometrics is obvious and continually expanding, but the improper taking or disclosing of such information can irreparably harm innocent employees or consumers. Some states have taken the initiative and passed laws solely dedicated to the protection of biometric information used in commercial settings. Other states and the federal government have worked biometric privacy safeguards into existing laws or have interpreted existing laws to cover biometric privacy. However, many states have not directly addressed commercial biometric privacy, and even the existing safeguards offer varying levels of incomplete protection.

---

[193] Kane Russell Logan Coleman, PC, *supra* note 153.

A federal law would offer uniform protection across the country, though the level of protection would depend on a myriad of factors including corporate lobbying, privacy lobbying, and state ideological differences. Regardless of the political hurdles on the track to ratification, Congress should aim for a biometric privacy law that is expansive and provides a private right of action so citizens do not have to rely on government actors for protection. A private right of action may lead to more litigation and disputes over legal technicalities, but those minor consequences are preferable to promulgating a feeble law that forces citizens to hope the attorney general decides to act when a complaint is made. When enforcement is handled solely by an attorney general's office, many cases will never be filed because of discretionary decisions and information gathering deficiencies.[194] Biometric information is invaluable to its owner, and the level of protection it is afforded should reflect that. Congress must take note of the how much inherent value biometric information holds and enact a federal law that fills current legislative gaps and safeguards the biometric data of American employees and consumers.

[194] Shukovsky, *supra* note 116.