YOUR BODY, YOUR DATA, BUT NOT YOUR RIGHT OF ACTION: SEEKING BALANCE IN FEDERAL BIOMETRIC PRIVACY LEGISLATION

Hannah Harper*

* Hannah Harper received her undergraduate political science degree from Michigan State University in 2016 and her Juris Doctor from George Mason University, Antonin Scalia Law School in 2021. Hannah was the Editor-in-Chief of the National Security Law Journal during the 2020-2021 academic year and would like to thank all NSLJ Editorial Boards, past and present, for their contributions to the journal's continued success.

I. INTRODUCTION

Biometrics created a world in which people walk around with their banking information displayed in the contours of their faces and their most intimate passwords etched in their fingertips. While these identifiers are increasingly used to facilitate secure transactions all over the globe, they are inherently accessible to everyone. One danger associated with the use of biometric identifiers is that they cannot be changed – they are a part of *you.* However, the unique characteristics of biometric identifiers make them increasingly valuable security tools for accessing electronic devices and preventing fraud. In response to the many privacy related concerns, several states have enacted legislation to protect biometric identifiers. However, these laws have generated concern regarding the ability of national and international businesses to comply with the different standards set by each state. This Comment advocates for a federal biometric privacy law focused on protecting biometric privacy without stifling industry.

Section II of this Comment will investigate the history of biometrics, its rise in popularity for secure transactions, and the current use of these identifiers by private entities. Additionally, Section II analyzes the laws in place to protect biometric privacy rights. Though no federal law governing biometric privacy currently exists, three states have enacted laws to provide safeguards for the use of biometric information by private entities. The first of these laws was

enacted by Illinois in 2008,[1] followed by Texas in 2009,[2] and Washington in 2017.[3] In 2020, Arizona,[4] Maryland,[5] New Hampshire,[6] South Carolina,[7] and West Virginia[8] introduced biometric privacy laws, but each of the associated bills have yet to pass.[9] California[10] and New York[11] also passed their own sets of comprehensive privacy legislation addressing the security of biometric information.[12] The discussion that follows will focus exclusively on state laws that have passed and gone into full effect. Associated litigation following the enactment of Illinois' Biometric Information Privacy Act (BIPA) will also be explored.

Section III of this Comment argues that the United States needs a comprehensive federal biometric privacy law and attempts to outline what that law should contain.[13] With our ever-increasing reliance on biometrics and lack of uniform protection of the associated privacy rights, the time for federal biometric privacy legislation is now. The federal law would have the benefit of hindsight and avoid mistakes made in state legislation, more effectively balancing the interests of individuals and private entities. Such federal legislation should

[1] 740 ILL. COMP. STAT. ANN. 14 / 5 (West 2021).
[2] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).
[3] WASH. REV. CODE ANN. § 19.375.020 (West 2021).
[4] H.B. 2728, 55th Leg., Reg. Sess. (Ariz. 2021).
[5] H.B. 307, 2020 Reg. Sess. (Md. 2020); S.B. 16, 2020 Reg. Sess. (Md. 2020).
[6] H.B. 1417, 2020 Reg. Sess. (N.H. 2020).
[7] H.B. 4812, Sess. 123 (S.C. 2020).
[8] H.B. 4106, Reg. Sess. 2020 (W. Va. 2020).
[9] Alicia A. Baiardo, *U.S. Biometrics Laws Part 1: An Overview of 2020*, MCGUIREWOODS (Feb. 1, 2021), https://www.passwordprotectedlaw.com/2021/02/u-s-biometrics-laws/ (all of the unenacted bills, with the exception of Arizona's, contained private rights of action for violations).
[10] CAL. CIV. CODE § 1798.100-.190 (West, 2021) (as amended by Assemb. B. 1355, Reg. Sess. (Cal. 2019)).
[11] N.Y. GEN. BUS. LAW § 899-bb (McKinney 2020).
[12] Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, THE NAT'L L. R. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.
[13] *See* S.4400, 116th Cong. (2020) (Since the drafting of this Comment, national biometric privacy legislation has been introduced in the Senate. This bill will be addressed in more detail in Section III.).

incorporate pieces of existing state laws while avoiding the pitfalls of stifling industry and floods of litigation. A balanced piece of federal legislation is more likely to pass and will uniformly implement the necessary biometric privacy protections.

II. BACKGROUND

A. What Are Biometrics?

Merriam-Webster defines biometrics as "the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity."[14] As the definition points out, there are two distinct types of biometric identifiers: physiological and behavioral.[15] Physiological biometric identifiers include fingerprints, the iris and retina, finger and hand shapes, face shape and geometry, and vein patterns.[16] Behavioral biometric identifiers include: "voice recognition, signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination), keystroke dynamics, the way objects are used, gait, the sound of steps, gestures, etc."[17]

B. A Brief History of Biometrics

Humans have been using and collecting biometric identifiers for centuries.[18] In addition to being excellent at facial recognition, human beings also recognize and use familiarity in speech and gait for identification purposes.[19] Although modern humans still rely on these types of recognition, population growth and territorial expansion necessitated new methods for identifying strangers.[20]

---

[14] *Biometrics*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/biometrics#h1.
[15] *What is Biometrics?*, GEMALTO, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (last updated Jun. 29, 2021).
[16] *Id.*
[17] *Id.*
[18] Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE, (Jan. 14, 2015), https://www.biometricupdate.com/201501/history-of-biometrics.
[19] *Id.*
[20] *Id.*

In 1883, Alphonse Bertillon's method for the identification of individuals was adopted by the Parisian police.[21] This method, "bertillonage," "identified individuals by measurements of the head and body, shape formations of the ear, eyebrow, mouth, eye, etc., individual markings such as tattoos and scars, and personality characteristics."[22] These measurements yielded a formula for a specific individual.[23] In 1884, this method was used to identify almost 250 offenders, prompting the adoption of bertillonage in other countries.[24] The method eventually faded as it was discovered that individuals could have identical measurements[25] and as fingerprinting became more prevalent.[26] Although these biometric measurements are not used as primary methods of identification today, some practices, such as the inventorying of scars, features, and tattoos, are reminiscent of bertillonage.[27]

In 1892, Sir Francis Galton published his book, *Fingerprints,* detailing his research on fingerprint classification.[28] The research focused on "patterns of arches, loops, and whorls."[29] In 1896, Sir Edward Henry furthered Galton's work and developed the "Henry Classification System."[30] Henry's system was "based on the direction, flow, pattern and other characteristics of the friction ridges in fingerprints."[31] Given these developments in the field, the first Fingerprint Bureau was established by Scotland Yard in 1901.[32] Prisons in New York began using fingerprints as a method of identification in 1903.[33] The Henry system provided law enforcement

[21] *Exhibition Biography of Alphonse Bertillon*, NAT'L LIBR. OF MED., https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/biographies/bertillon.html (last updated June 5, 2014) [hereinafter *Exhibition Biography*].
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] Mayhew, *supra* note 18.
[26] *Exhibition Biography*, *supra* note 21.
[27] *Id.*
[28] Stephanie Watson, *How Fingerprinting Works*, HOWSTUFFWORKS.COM (Mar. 24, 2008), https://science.howstuffworks.com/fingerprinting.htm.
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*

with a method for classification and identification of fingerprints, but the system of manual collection and comparison of fingerprint cards became unmanageable with time.[34]

On contract with the FBI, the National Institute of Science and Technology began exploring automating the process.[35] The resulting system was called "AFIS" – Automated Fingerprint Identification System.[36] AFIS expedited the identification process and enabled law enforcement to solve crimes more efficiently than ever before.[37] In a subsequent improvement to AFIS, the ability to identify palm prints was added.[38]

In 1999, the FBI implemented the Integrated Automated Fingerprint Identification System (IAFIS).[39] IAFIS has been gradually replaced by a new system, Next Generation Identification (NGI).[40] NGI's purpose is described as "improv[ing] the efficiency and accuracy of biometric services to address evolving local, state, tribal, federal, national, and international criminal justice requirements."[41] NGI combines multiple biometric identifier capabilities such as fingerprint identification, facial recognition, iris recognition, and palm print identification.[42]

While fingerprinting was being developed and refined, iris patterns were also suggested as a means of identification in 1936 by Dr. Frank Burch.[43] Iris recognition algorithms were patented in 1994.[44] This type of biometric identifier is used for "access control for high security installations, credit card usage verification, and

[34] Watson, *supra* note 28.
[35] *A History of AFIS*, SECUREIDNEWS.COM, (Dec. 2, 2014) https://www.secureidnews.com/news-item/a-history-of-afis/.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Next Generation Identification*, FBI.GOV, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] Stephen Mayhew, *Explainer: Iris Recognition*, BIOMETRIC UPDATE, https://www.biometricupdate.com/201206/explainer-iris-recognition.
[44] *Id.*

employee identification."[45] Using the iris for identification purposes gained popularity due to its stability, ease of capture, and unique qualities.[46]

In addition to using fingerprints and irises as identifiers, the first semi-automatic facial recognition was developed in the 1960s by Woodrow Wilson Bledsoe.[47] His device, the RAND tablet, involved inputting "horizontal and vertical coordinates on a grid using a stylus that emitted electromagnetic pulses."[48] The locations of facial features were recorded and uploaded to a database.[49] From that database, similar facial features could be retrieved upon the introduction of a new photograph.[50]

Facial recognition has come a long way since the 1960s.[51] In 2012, the Federal Trade Commission (FTC) issued a report titled, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*.[52] The report highlighted privacy concerns posed by the relatively new use of facial recognition for commercial purposes.[53] The recommendations in the report included keeping consumer privacy in mind, developing safeguards and retention/destruction policies, and

[45] Seifedine Kadry & Smaili Khaled, *A Design and Implementation of a Wireless Iris Recognition Attendance Management System*, 36 INFO. TECH. & CONTROL 323, 323 (2007) https://pdfs.semanticscholar.org/c2ff/b61af594701f9596784f910f5b349af083c8.pdf.
[46] *Id.*
[47] Dhairya Parikh, *Advancements in Computer Based Facial Recognition Systems: From the RAND Tablet to Differentiating Identical Twins*, MEDIUM, (June 30, 2018), https://medium.com/coinmonks/from-the-rand-tablet-to-differentiating-identical-twins-aa4ba6031bb0.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] Press Release, FTC, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies, (Oct. 22, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition [hereinafter FTC Press Release].
[53] *Id.*

remaining cognizant to avoid gathering information of a sensitive nature – like the facial recognition data of minors.[54]

Additionally, the FTC report suggested that companies using facial recognition technology should give consumers adequate notice and the ability to avoid collection if they so choose.[55] Specifically directed at social media, the FTC warned that clear notice should be provided about the function of a facial recognition feature and the collection and use of the data.[56] Lastly, the FTC recommended requiring affirmative consent in two scenarios: when the actual use differs from the reason represented during collection, and when "identify[ing] anonymous images of a consumer to someone who could not otherwise identify him or her."[57]

C. Private Sector Use

While many uses of biometric identifiers have ties to law enforcement, this Comment will focus solely on private sector use. As the 2012 FTC report[58] indicated, some of the most contentious biometric privacy issues stem from social media. For example, "[s]ocial media and other companies frequently use technologies that create facial geometry templates . . . from photographs. Companies use these technologies to identify and/or group together photographs of the same person—associations they then use for internal purposes and/or for customer offerings."[59] If you have a Facebook account, you are likely familiar with the process being described.[60] But Facebook is by no means the only private entity using biometric information –

[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] FTC Press Release, *supra* note 52.
[59] Lara Tumeh, *Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law*, BLOOMBERG LAW, (Oct. 12, 2017), https://www.bloomberglaw.com/document/XAOH0ETG000000?bna_news_filter=privacy-and-data-security&jcsearch=BNA%25200000015e7763d2bcaf7ff7e737110003#jcite.
[60] FACEBOOK, https://www.facebook.com/help/122175507864081 ("Face recognition is used to analyze the photos and videos we think you're in on Facebook, such as your profile picture and photos and videos that you've been tagged in, to make a unique number for you, called a template.").

businesses from tanning salons[61] to locker rentals[62] to technology companies[63] use this sensitive information to increase efficiency, security, and identification accuracy. For the purpose of this Comment, private sector use encompasses practices by social media companies, as well as businesses using biometric identifiers for secure transactions, identity verification, efficiency, or a combination of these purposes.

D. Gaining Popularity Despite Concerns

So, why is there concern over private entities' increasing reliance on biometrics? Biometric identifiers are made up of parts of *you* – they cannot be changed.[64] If your Facebook is hacked, you change the password; if your credit card is stolen, you should deactivate the card. However, if your biometric identifiers are compromised, you cannot easily alter your fingerprints, iris patterns, or facial geometry.[65]

Another issue with the use of biometric identifiers is that they are visible and, in some cases, accessible by everyone – "[s]ome pieces of your physical identity can be duplicated. For example, a criminal can . . . copy your fingerprints from a glass you leave at a cafe. This information could potentially be used to hack into your devices or accounts."[66] Additionally, like any data, biometrics are sometimes

[61] Sekura v. Krishna Schaumburg Tan, Inc., 115 N.E.3d 1080, 1084 (IL App. Ct. 2018) (alleging a tanning salon violated Illinois' Biometric Information Privacy Act (BIPA) when it collected fingerprints without disclosing retention and destruction policies).
[62] McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016) (involving lockers in public areas that used fingerprints of renters as keys).
[63] Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019); Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017); Gullen v. Facebook.com, Inc., No. 15-cv-7681, 2016 WL 245910 (N.D. Ill. Jan. 21, 2016).
[64] Kim Porter, *Biometics and Biometric Data: What is it and is it Secure?*, NORTON (Feb. 8, 2019), https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html.
[65] *Id.*
[66] *Id.*

stored in databases; as such, your biometric identifiers could be accessed by bad actors in the event of a data breach.[67]

Despite the relevant concerns, biometrics continue to gain popularity for identification purposes because they provide "an exceptionally secure way to log in to your devices and various services."[68] Any person who has owned multiple generations of the iPhone will have noticed the gradual progression from four-digit passcodes, to six-digit passcodes, to thumbprint scans, and finally, to facial recognition. It used to be easy to glance over at someone typing in their passcode, potentially enabling access to the device. Such means of access is becoming less common thanks to biometrics. While Apple still requires entering a password after the phone restarts or after too many failed facial recognition attempts, the susceptibility of password cracking by onlookers has been greatly reduced.[69]

In essence, the very thing that makes biometric identifiers attractive for verification purposes also presents the most challenging problem – these unique identifiers cannot be changed.[70]

E. State Biometric Privacy Laws

As mentioned in Section I, there is no federal biometric privacy law. Considering this absence, three states have successfully enacted their own biometric privacy laws and several others are considering similar legislation or seek to address biometrics indirectly through broader privacy legislation.[71] The discussion of the state statutes will proceed in chronological order based on the date of

[67] *Id.* (noting that stored biometric information might be at greater risk because it cannot be changed in the same way that breached passcodes can).
[68] *Id.*
[69] *Id.*
[70] Porter, *supra* note 64.
[71] Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 648 (2018) (identifying Illinois, Texas, and Washington as states with specific biometric privacy laws and stating "Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming have regulated the collection of biometric information by defining 'personal information' in data security breach notification laws to include types of biometric data."); *see also* Baiardo, *supra* note 9.

enactment: Illinois,[72] Texas,[73] then Washington.[74] A review of the resulting litigation will follow the discussion of Illinois' statute. Additionally, this section contains summaries of certain portions of the California Consumer Privacy Act (CCPA) and New York's SHIELD Act addressing biometrics.[75]

1. Illinois

In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA) in response to the increased usage of and dependency on biometric information in the modern world.[76] BIPA's definition of "biometric identifier" includes: "retina or iris scan[s], fingerprint[s], voiceprint[s], or scan[s] of hand or face geometry."[77] It expressly excludes "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."[78]

The Act requires private entities "in possession of biometric identifiers or biometric information" to have a publicly available written policy detailing retention and destruction procedures.[79] Pursuant to BIPA, destruction must take place "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."[80]

The Act also requires the private entity to inform the individual or their representative in writing about the collection or storage of biometric identifiers, including purpose and length of use.[81]

---

[72] 740 ILL. COMP. STAT. ANN. 14/5 (West 2021).
[73] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).
[74] WASH. REV. CODE ANN. § 19.375.020 (West 2021).
[75] CAL. CIV. CODE § 1798.100-.190 (West 2021) (as amended by Assemb. B. 1355, Reg. Sess. (Cal. 2019)); N.Y. GEN. BUS. LAW § 899-bb (McKinney 2020).
[76] 740 ILL. COMP. STAT. ANN. 14/5 (West 2021).
[77] 740 ILL. COMP. STAT. ANN. 14/10 (West 2021).
[78] *Id.*
[79] 740 ILL. COMP. STAT. ANN. 14/20 (West 2021).
[80] *Id.*
[81] *Id.*

Private entities must receive a written release if they wish to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information."[82] BIPA prohibits private entities from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information."[83]

Additionally, the Act places stringent limitations on private entities' ability to disclose or disseminate the biometric information they have obtained.[84] To prevent inadvertent disclosure, BIPA requires private entities to use a reasonable industry standard of care when storing and transmitting these identifiers and mandates the use of higher safety standards than would be used in the protection of other sensitive information.[85]

The defining feature of BIPA, as opposed to the biometric privacy legislation of other states, is that it creates a private right of action.[86] Coupled with other stringent requirements, like written consent and banning the sale of biometric identifiers, BIPA primarily serves the interests of individuals at the expense of private entities.[87] By creating a private right of action and including facial and hand geometry scans in its definition of biometrics, BIPA's enactment spurred a "flurry of class action litigation."[88] The BIPA cases will be discussed before addressing other state biometric privacy statutes, as it is plausible that the post-BIPA litigation had some impact on subsequent decisions not to include private rights of action in the other laws.

a. Litigation Post-BIPA – Rosenbach v. Six Flags

Potentially the most significant post-BIPA decision was *Rosenbach v. Six Flags*.[89] Since 2014, Six Flags, the operator of an

[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] 740 ILL. COMP. STAT. ANN. 14/20 (West 2021).
[86] *Id.*
[87] Tumeh, *supra* note 59.
[88] *Id.*
[89] Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1200 (Ill. 2019).

amusement park in Illinois, had been using fingerprints to issue park passes.[90] The prints were scanned and stored to expedite customer verification.[91] This particular system was adopted for efficiency and to "eliminate[] lost revenue due to fraud or park entry with someone else's pass."[92] In preparation for a school field trip, Stacy Rosenbach purchased a season pass for her 14-year-old son online.[93] While the purchase could be made online, the process also required an in-person scan of his thumbprint and the receipt of a season pass card.[94] Six Flags failed to inform the parties about the collection of the thumbprint, its purpose, or use. Neither party signed a written release or gave written consent "to the collection, storage, use [sic] sale, lease, dissemination, disclosure, redisclosure, or trade of, or for [defendants] to otherwise profit from" the biometric information obtained. [95] At the time of the lawsuit, Six Flags remained in possession of the thumbprint and had no publicly available policy detailing use, retention, or destruction schedules.[96]

Rosenbach filed suit on behalf of her son under BIPA, which provides a right of action for "any person 'aggrieved' by a violation of the Act's provisions."[97] Damages were sought on three grounds: (1) failing to inform of the collection in writing, (2) failing to provide purposes of collection and length of use, and (3) failing to obtain a written release prior to collection.[98]

Six Flags argued Rosenbach lacked standing and that BIPA's purpose was to protect those who "sustained some actual damage, beyond violation of the rights conferred by the statute."[99] The court rejected this argument and held that the plaintiffs did not need to show additional harm to sue under BIPA.[100] The improper collection

[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Rosenbach,* 129 N.E.3d at 1201.
[96] *Id.*
[97] *Id.* (quoting 740 ILL. COMP. STAT. ANN. 14/20).
[98] *Id.*
[99] *Id.* at 1204.
[100] *Id.* at 1207.

methods used by Six Flags implicated statutory harm and posed sufficient grounds for suit.[101]

After this decision was issued in January of 2019, Holland & Knight, an international law firm, issued an alert about the rise of class action lawsuits post-BIPA.[102] The alert declared that the *Rosenbach* decision "opened the door for increased filing of BIPA class actions, most of which are directed at employers that utilize fingerprinting technology for timekeeping purposes."[103]

b. Litigation Post-BIPA – Patel v. Facebook

In a subsequent case, *Patel v. Facebook*, the Ninth Circuit ruled on the issue of Article III standing under BIPA.[104] Facebook users brought this class action against the social media giant for alleged violations of BIPA.[105] The plaintiffs claimed Facebook's facial-recognition technology – used in its "Tag Suggestions" feature – violated Illinois law because it did not require a written release and did not set forth a compliant retention policy.[106]

In its opinion, the court detailed a two-step process used to determine Article III standing when a plaintiff incurs solely intangible injuries.[107] The test evaluates the presence of concrete interests at stake and whether the violations alleged present a material risk of harm to those interests.[108] Addressing the first prong of the test, the Ninth Circuit used recent Supreme Court Fourth Amendment jurisprudence to determine that the "invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been

---

[101] *Rosenbach,* 129 N.E.3d at 1207.
[102] Richard R. Winter et al., *BIPA Update: Class Actions on the Rise in Illinois Courts*, HOLLAND & KNIGHT (July 22, 2019), https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts.
[103] *Id.*
[104] *Patel,* 932 F.3d at 1264.
[105] *Id.* at 1267.
[106] *Id.* at 1267-68.
[107] *Id.* at 1270-71.
[108] *Id.*

regarded as providing a basis for a lawsuit . . .'"[109] Addressing the second part of the test, the Ninth Circuit cited the Supreme Court's decision in *Spokeo, Inc. v. Robins* and reiterated that a "violation of a statutory right that protects against 'the risk of real harm' may be sufficient to constitute injury-in-fact, and under those circumstances a plaintiff 'need not allege any additional harm.'"[110]

Ultimately, the court ruled BIPA was established to protect the plaintiffs' concrete biometric privacy interests, and the violations alleged presented a material risk of harm to those interests.[111] The Ninth Circuit affirmed the lower court's denial of Facebook's motion to dismiss for lack of Article III standing and certified the class.[112]

2. Texas

In 2009, Texas enacted a statute to protect biometric privacy rights. The statute defines "biometric identifier" as including "retina or iris scan, fingerprint, voiceprint, or record[ing] of hand or face geometry."[113] The Act prohibits the capture of biometric identifiers for commercial purposes unless (1) the individual has been informed and (2) gives consent.[114] Captured identifiers may not be sold, leased, or disclosed, unless consent is given for identification purposes in case of death or disappearance; it completes a financial transaction authorized or requested by the individual; disclosure is required or permitted by federal or state statute; or it is pursuant to a warrant.[115]

To protect biometric identifiers from disclosure, possessors must use a reasonable care standard "that is the same as or more protective than the manner in which . . . other confidential information" is stored, transmitted, and protected.[116] The retention provisions of the statute mandate destruction of "the biometric

[109] *Patel,* 932 F.3d at 1271-73 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).
[110] *Id.* at 1270 (quoting *Spokeo*, 136 S. Ct. at 1549).
[111] *Id.* at 1274-75.
[112] *Id.* at 1275, 1277.
[113] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).
[114] *Id.*
[115] *Id.*
[116] *Id.*

identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires."[117] An exception to this provision concerns identifiers "used in connection with an instrument or document" that another law requires to be maintained for longer than the provision in this Act.[118] If an employer collects the information for security purposes, the purpose for collection expires upon termination of employment.[119]

The Texas statute does not create a private right of action but instead provides that the State Attorney General "may bring an action to recover the civil penalty."[120] The civil penalty is not to exceed $25,000 per violation.[121]

3. Washington

In 2017, Washington became the third state to pass a biometric privacy law.[122] The statute defines "biometric identifiers" as: "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[123] The statute explicitly excepts photographs, video, and audio recordings from its definition.[124]

In enacting the statute, the Washington legislature focused on lack of knowledge and consent as a major concern with biometric data collection and its subsequent use for marketing purposes.[125] The Act addressed these concerns by requiring businesses in possession of this data to "disclose how it uses that biometric data, and provide notice to

[117] *Id.*
[118] *Id.*
[119] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).
[120] *Id.*
[121] *Id.*
[122] WASH. REV. CODE ANN. § 19.375.020 (West 2021).
[123] WASH. REV. CODE ANN. § 19.375.010 (West 2021).
[124] *Id.*
[125] WASH. REV. CODE ANN. § 19.375.900 (West 2021).

and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database."[126]

Before using biometric identifiers for commercial purposes, notice and consent must be given, or a mechanism must be provided "to prevent the subsequent use of a biometric identifier for a commercial purpose."[127] The statute does not define what notice and consent consist of, instead, these requirements are considered "context-dependent."[128]

In the absence of consent, a person is prohibited from selling, leasing, or disclosing the identifier for a commercial purpose unless it: (1) adheres to the requisite notice, consent, security, and retention provisions; (2) is "necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual"; (3) is "made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent" provisions; (4) "is required or authorized by a federal or state statute, or court order"; or (5) is made in preparation for litigation or judicial process.[129]

Lastly, the Washington legislature expressly declined to create a private right of action – stating, "[t]his chapter may be enforced solely by the attorney general under the consumer protection act."[130]

F. Comparing and Contrasting the Statutory Requirements

Unsurprisingly, many of the states' restrictions on the commercial use of biometric information overlap. For example, each state requires notice and consent to collect biometric identifiers, reasonable security measures, and imposes guidelines for disclosure,

[126] *Id.*
[127] WASH. REV. CODE ANN. § 19.375.020 (West 2021).
[128] *Id.*
[129] *Id.*
[130] WASH. REV. CODE ANN. § 19.375.030 (West 2021).

retention, and destruction.[131] While these general mandates appear in each statute, the details or definitions vary among the individual statutes.[132] Specifically related to disclosure, each statute permits a collecting entity to disclose biometric identifiers when: (1) consented to, (2) required by law, (3) pursuant to a warrant,[133] subpoena,[134] or court order,[135] and (4) necessary to complete authorized financial transactions.[136]

Despite the overlap in provisions and stated objectives, the Texas and Washington statutes noticeably differ from BIPA in two important ways. The first is that BIPA broadly prohibits the sale of biometric identifiers[137] while the Texas and Washington statutes permit sale under certain circumstances.[138] The second is that while BIPA creates a private right of action,[139] neither the Texas nor Washington statutes contain such a provision.[140] Two reasonable inferences may be drawn from these significant legislative differences. The first is that Texas and Washington each may have wanted their legislation to be more business-friendly than the heavily individual-focused BIPA. The second is that Texas and Washington both may have wanted to avoid the flood of litigation that BIPA's private right of action unleashed.[141]

G. The California Consumer Privacy Act of 2018 (CCPA)

While not exclusively a statute about biometric privacy rights, the California Consumer Privacy Act (CCPA) addresses and protects

---

[131] Tumeh, *supra* note 59 (noting, however, that Illinois is the only state which clearly defines what its notice and consent requirements are).
[132] *Id.*
[133] *Id.* (noting that Illinois and Texas include disclosure pursuant to a warrant).
[134] *Id.* (noting that Washington permits disclosure pursuant to a court order).
[135] *Id.* (noting that Illinois permits disclosure pursuant to a subpoena).
[136] *Id.*
[137] 740 ILL. COMP. STAT. ANN. 14/15 (West 2021).
[138] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021); WASH. REV. CODE ANN. § 19.375.020 (West 2021).
[139] 740 ILL. COMP. STAT. ANN. 14/15 (West 2021).
[140] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021); WASH. REV. CODE ANN. § 19.375.030 (West 2021).
[141] Winter et al., *supra* note 102.

biometrics within its scope. The CCPA defines biometric information as:

> . . . an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.[142]

Due to the long and complicated history of the CCPA, understanding the rights of action established by the legislation is no easy task. Most suits for CCPA violations may only be brought by the State Attorney General.[143] However, "the CCPA authorizes a private right of action only for breaches involving the nonredacted and unencrypted 'personal information' of California consumers."[144] One commentator observed: "[r]estriction of the private right of action was instrumental to the passage of the CCPA in the first place. This is because the legislators understood the power of unrestricted lawsuits."[145] As evidenced by the narrowly created private right of

[142] CAL. CIV. CODE § 1798.140 (West 2021).
[143] Theodore F. Claypoole, *Private Right of Action vs. Statutory Damages. Which Has More Impact?*, THE NAT'L LAW REVIEW (Aug. 2, 2019), https://www.natlawreview.com/article/private-right-action-vs-statutory-damages-which-has-more-impact.
[144] Jonathan (Yoni) Schenker et al., *A Closer Look at the CCPA's Private Right of Action and Statutory Damages*, LEXOLOGY (Aug. 22, 2019), https://www.lexology.com/library/detail.aspx?g=f2aed27f-adee-47fd-8b0a-f0bbb116307f; *see also* https://oag.ca.gov/privacy/ccpa (Stating in response to the Frequently Asked Question (FAQ), "What kind of data breach can I sue a business for under the CCPA?" – "You can only sue businesses under the CCPA if certain conditions are met . . . The personal information must have been stolen in nonencrypted and nonredacted form.").
[145] Claypoole, *supra* note 143.

action in the CCPA, it is clear that preventing a flood of litigation was on the mind of its legislators. California likely wanted to avoid "every lapse in security or clever phishing attack spawn[ing] a set of class action lawsuits."[146] The narrow private right of action and the complicated legislative history of the CCPA will be discussed in detail in a later section.

H. New York's SHIELD Act

Like the CCPA, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) is not strictly a piece of biometric privacy legislation, rather it has the broad goal "of strengthening protection for New York residents against data breaches affecting their private information, [it] imposes more expansive data security and updates its existing data breach notification requirements."[147] Within its definition of "private information," the SHIELD Act includes: "biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity . . . ."[148]

Although similar to the CCPA in some ways, "the SHIELD Act does not create affirmative rights for New York residents," nor does it create a private right of action.[149] Despite this, "the Attorney General may bring an action to enjoin violations of the law and obtain civil penalties."[150] If the violation was unintentional or the result of recklessness, the remedy is actual damages.[151] If the violation is

[146] *Id.*
[147] Joseph J. Lazzarotti, Jason C. Gavejian, Damon W. Silver, Mary T. Costigan, Delonie A. Plummer, *New York SHIELD Act FAQs*, THE NAT'L L. REV. (Mar. 11, 2020), https://www.natlawreview.com/article/new-york-shield-act-faqs.
[148] *Id.*
[149] *Id.*
[150] *Id.*
[151] *Id.*

reckless, "a court may impose penalties of the greater of $5,000 or up to $20 per instance with a cap of $250,000."[152]

III. ANALYSIS

Authoritative legal commentators concur almost unanimously that a federal biometric privacy law is fundamentally necessary. However, disagreement tends to arise concerning the specific provisions to include in such federal legislation. Subsection A presents the argument detailing why the United States needs to protect biometric privacy rights at the federal level. Subsection B presents the rationale of those who advocate for the inclusion of a private right of action in the federal legislation. Subsection C identifies three primary concerns with those proposals and explains why a federal biometric privacy law should not include a private right of action. Lastly, Subsection D discusses what federal legislation on this topic should include and why striking a balance between the rights of individuals and businesses is important.

A. Why We Need Federal Biometric Privacy Legislation

Privacy law at the federal level has been described as "a patchwork of statutes" and insufficient for the purposes of protection or guidance.[153] The fact that the United States is a "world leader in data-driven business" makes the dearth of federal law regulating private sector collection, storage, and use of biometric identifiers something of a mystery.[154]

Currently, federal law regulates only specific industries' uses of personal data.[155] This limited, industry-specific protection of data

---

[152] *Id.*

[153] Zimmerman, *supra* note 71, at 643–44.

[154] *Id.*

[155] *Id.* at 644; *see also* Lauren Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C. L. REV. 349, 379 (2019) (stating "regulations at the federal level are industry-specific and inconsistent across sectors.").

privacy rights is called the "sectoral approach."[156] The piecemeal nature of the sectoral approach necessarily creates both gaps and overlap.[157] With the narrow exception of the Health Insurance Portability and Accountability Act (HIPAA), no federal statute currently regulates private sector use of biometrics.[158] Not only would federal biometric privacy law need to provide the protection required of such sensitive data, but it must also establish clear guidelines for businesses to follow.[159]

One of the goals of enacting such a law would be to establish nationwide, uniform regulations for businesses' use of biometric data.[160] Without a federal biometric privacy law, "businesses operating across the U.S. will need to understand each state's requirements and how they overlap and differ from those of other states."[161] Illinois' BIPA has been described as the most "consumer-protective," while the Texas and Washington statutes lean more toward the side of protecting commercial interests.[162] Businesses operating in more than one of these states must endeavor to navigate the varying requirements of each.[163] Federal legislation in the area of biometrics should seek to strike a balance between consumer privacy and commercial interests.

B. The Argument for a Private Right of Action

Even those who support the inclusion of a private right of action acknowledge the deluge of cases that will inevitably follow.[164] A

---

[156] Zimmerman, *supra* note 71, at 644–45 (2018); *see also* Blake Benson, *Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy*, 19 N.C.J.L. & TECH. ON. 161, 186 (2018) (describing the sectoral process as "simultaneously too restrictive and not restrictive enough").

[157] Benson, *supra* note 156, at 186.

[158] *See* Zimmerman, *supra* note 71, at 645 (stating that HIPAA is the only "direct regulation of biometric information collected by private entities"); *see also* Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 647 (2019).

[159] Benson, *supra* note 156, at 186.

[160] *Id.*

[161] Tumeh, *supra* note 59.

[162] *Id.*

[163] *Id.*

[164] Benson, *supra* note 156, at 190.

principal argument in defense of the private right of action is that statutory definitions and comprehensiveness will help minimize the litigation.[165] While this Comment supports the inclusion of more comprehensive definitions, it is unlikely that these additional definitions, standing alone, would be enough to temper the litigation. Another argument is that private citizens need to be able to enforce their rights "without relying on an Attorney General's office."[166] To support this argument, some legal commentators believe that biometric privacy cases will be "selectively pursued based on the discretion of a small group of attorneys."[167]

While the selective pursuit of cases is an inherent risk in statutes entrusting enforcement to the Attorney General, this is not a new concept, nor is it one with which to be particularly concerned. Historically, the Attorney General has been charged with enforcing such important statutes as the Americans with Disabilities Act[168] and the Voting Rights Act.[169]

Congress is ultimately best situated to determine where the enforcement power of federal biometric privacy legislation should fall. However, justifying the inclusion of a private right of action by arguing that the Attorney General would be incapable of adequately protecting consumers' biometric privacy rights ultimately fails as a weak argument.

C. The Argument Against a Private Right of Action

This section presents three primary arguments against including a private right of action in a federal biometric privacy law. First, creating a private right of action would lead to a flood of class action litigation – like in the case of BIPA.[170] Second, unduly burdening the technological developments and security procedures of

[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] 42 U.S.C. § 12101 (2018).
[169] 52 U.S.C. § 10301 (2018).
[170] Winter et al., *supra* note 102.

businesses would stifle industry. Finally, post-BIPA, a balanced piece of legislation is more likely to pass.

1. Flood of Litigation

A Holland & Knight alert issued on July 22, 2019, stated that 213 BIPA cases had been filed in 2018 and 2019.[171] The alert characterized most of the cases as class actions "directed at employers utilizing fingerprint technology for timekeeping purposes."[172] This alert was joined by many others issued by law firms and legal news sources about the substantial litigation resulting from BIPA and, specifically, the *Rosenbach*[173] decision.[174] Following this tremendous increase in litigation, Illinois' Senate introduced a bill that would delete the language creating a private right of action in BIPA.[175] The most recent action on this bill was when it was re-referred to Assignments on March 28, 2019.[176] As such, the fate of BIPA's private right of action remains uncertain.

For those who would praise BIPA's current inclusion of a private right of action, it may be useful to consider how it actually works. The recovery is capped at $1,000 for negligent violations and $5,000 for intentional violations unless the litigant can prove actual damages in excess of those amounts.[177] Given the sheer expense of

[171] *Id.*
[172] *Id.*
[173] *Rosenbach*, 129 N.E.3d at 1200.
[174] *See, e.g.*, *Illinois Biometric Information Privacy Act (BIPA)*, LEWIS BRISBOIS, https://lewisbrisbois.com/practices/bipa-illinois-biometric-information-privacy-act; *Biometric Information Privacy Act*, HINSHAW, https://www.hinshawlaw.com/services-biometric-information-privacy-act.html; Gerald L. Maatman, Jr. et al., *Biometric Privacy Class Actions By The Numbers: Analyzing Illinois' Hottest Class Action Trend*, SEYFARTH SHAW LLP (June 28, 2019), https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/; Steven Grimes, *Biometric Privacy Litigation: The Next Class Action Battleground*, BIG LAW BUSINESS (Jan. 9, 2018), https://biglawbusiness.com/biometric-privacy-litigation-the-next-class-action-battleground.
[175] Winter et al., *supra* note 102.
[176] S.B. 2134, 101st Gen. Assemb., Reg. Sess. (Ill. 2019).
[177] Kirill Levashov, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164, 177 (2013).

litigation and the inherent difficulty in proving actual damages exceeding that amount, the BIPA private right of action may not be what it appears to be.[178]

Regardless of the way it functions, it is clear that the inclusion of the private right of action in BIPA resulted in a substantial amount of litigation. Such an inclusion should be viewed as a failed experiment not to be replicated at the federal level. It is telling that neither of the subsequently enacted state statutes included a private right of action[179] and that the Illinois legislature affirmatively made some effort to delete the creation language from BIPA.[180] As such, biometric privacy legislation at the federal level should learn from Illinois' experience and exclude a private right of action for violations.

2. Stifling Industry

In a criticism of BIPA, one commentator observed that it "provides a nearly unlimited scope of regulation that could stymie growth of the data security industry and thwart the purpose of many new technologies that provide security through biometric identification."[181] This commentator gave the example of Nest, a smart doorbell company.[182] The Nest doorbell has a feature capable of learning faces.[183] This feature has obvious security purposes, but it would be impossible to get the consent required under BIPA from front porch visitors.[184] For these reasons, Nest chose to disable the learning feature in Illinois.[185]

Another example comes from Google's Arts & Culture app.[186] This app allowed users to match uploaded selfies with look-alike

[178] *Id.*
[179] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021); WASH. REV. CODE ANN. § 19.375.030 (West 2021).
[180] S.B. 2134, 101st Gen. Assemb., Reg. Sess. (Ill. 2019).
[181] Stewart, *supra* note 155, at 380.
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] Ally Marotti, *Illinois Supreme Court Rules Against Six Flags in Lawsuit Over Fingerprint Scans. Here's Why Facebook and Google Care.*, CHICAGO TRIBUNE (Jan.

famous works of art.[187] However, this feature was unavailable to Illinois residents.[188] One article on the subject mused, "it's likely because Illinois has one of the nation's most strict laws on the use of biometrics, which include facial, fingerprint and iris scans."[189] Should federal legislation be modeled on the industry-restrictive BIPA, negative implications for technological advancements would surely follow.

One way to remedy this issue would be for federal legislation to focus specifically on the misuse of biometric information. This is a necessary specification because BIPA was drafted in a manner that permits standing for plaintiffs on the basis of preventing individual invasions of privacy without any proof of actual misuse.[190] In fact, BIPA "authorizes private citizens to sue for the alleged misuse of their biometric data before any unauthorized access or data breach."[191] Thus, under BIPA, whether the data was misused in any way is irrelevant as long as a personal privacy concern is stated.[192] Federal biometric privacy legislation should take its cue instead from the CCPA Assembly Bill 1355, signed by Governor Newsom on October 11, 2019:

> Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information

25, 2019, 10:30 AM), https://www.chicagotribune.com/business/ct-biz-six-flags-biometrics-lawsuit-20190125-story.html.

[187] *Id.*

[188] *Id.*

[189] Ally Marotti, *Google's Art Selfies Aren't Available in Illinois. Here's Why.*, CHICAGO TRIBUNE (Jan. 17, 2018, 7:00 AM), https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html.

[190] *See Rosenbach*, 129 N.E.3d at 1207.

[191] Charles L. Insler, *How to Tackle Litigation under the Biometric Information Privacy Act*, 35 THE COMPUT. & INTERNET LAWYER 1, 2 (No. 12, Dec. 2018), https://www.heplerbroom.com/cmss_files/attachmentlibrary/News/2018-11-27---ICIL_1218_Insler.pdf.

[192] *See id.*

> to protect the personal information may institute a civil action . . . .[193]

Although this section grants a narrow private right of action in the event of a data breach,[194] the motivation behind the grant is what the federal legislation should adopt – some type of misuse or improper disclosure as a trigger. Without the exposure of nonencrypted and nonredacted data, there exists no private right of action under the CCPA.[195] In other words, to exercise a private right of action under the CCPA, something must have been done incorrectly, or the risk for improper disclosure of personal information must be very great.[196]

By avoiding the overly broad language of BIPA and making misuse or improper disclosure the triggering event for suit under the federal statute, federal biometric privacy legislation will avoid stifling the data security industry and the development of new technology while also protecting the privacy of individuals.

3. Balance and the Likelihood of Passage

It is unlikely that federal biometric privacy legislation *including* a private right of action would be enacted. However, with increasing reliance on biometric information for all sorts of transactions and security features, this type of legislation is imperative to adequately protect the security of such sensitive data on a national level. To achieve the goal of passing a law to protect that privacy, it is necessary to strike the proper balance between the interests of businesses and individuals.

It appears obvious that, post-BIPA, the inclusion of a private right of action in biometric privacy legislation at the state level is, at the very least, unpopular. In the years since its enactment, the Illinois legislature has attempted to dismantle the private right of action

[193] Assemb. B. 1355, Reg. Sess. (Cal. 2019).
[194] *Id.*
[195] *California Shakes Up Data Privacy for 2020*, MCCARTER & ENGLISH (Nov. 13, 2019), https://www.jdsupra.com/legalnews/california-shakes-up-data-privacy-for-86577/ [hereinafter CCPA Article].
[196] Assemb. B. 1355, Reg. Sess. (Cal. 2019).

creation language in BIPA,[197] and both state statutes passed after BIPA entrusted the right to bring claims to the states' attorneys general.[198]

California's new privacy legislation, the CCPA, originally included a broader private right of action but was narrowed in subsequent amendments.[199] After SB 561 was blocked in the California Senate, technology companies "claimed victory" in the private right of action debacle.[200] This amendment to the CCPA would have "expressly grant[ed] plaintiffs the right to sue for all CCPA violations and most likely set in motion a wave of litigation" in early-2020.[201] By blocking the bill, the original, narrow private right of action in the event of a data breach is what remains.[202] Commentators called this "a positive development for businesses scrambling to comply with CCPA."[203]

In the CCPA battle, those pushing for more restrictive language faced off against "the California Chamber of Commerce, as well as leading technology lobbying firms that represent the likes of Facebook, Google, Amazon, and Apple."[204] While federal and state legislatures should not bend entirely to the will of lobbying firms and technology companies, their interests are an important consideration

---

[197] Meghan C. O'Connor et al., *Illinois Introduces Bills to Amend BIPA Taking Away Private Right of Action and Adding ECGs*, QUARLES & BRADY LLP (April 25, 2019), https://www.quarles.com/publications/illinois-introduces-bills-to-amend-bipa-taking-away-private-right-of-action-and-adding-ecgs/.

[198] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021); WASH. REV. CODE ANN. § 19.375.030 (West 2021).

[199] CCPA Article, *supra* note 195.

[200] *Expanded CCPA Private Right of Action Fails, But Threat of Private CCPA Claims May Not Be Over*, INFOLAWGROUP (May 22, 2019), https://www.infolawgroup.com/blog/2019/5/22/expanded-ccpa-private-right-of-action-fails-but-threat-of-private-ccpa-claims-may-not-be-over [hereinafter ILG Article].

[201] *Id.*

[202] Christina Kroll, *CCPA: The California Senate is Not Ready to Expand the Consumer Right of Action*, PROSKAUER (May 17, 2019), https://privacylaw.proskauer.com/2019/05/articles/california/the-california-senate-is-not-ready-to-expand-the-consumer-right-of-action/.

[203] ILG Article, *supra* note 200.

[204] Issie Lapowsky, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (April 29, 2019, 3:09 PM), https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/.

and cannot be overlooked. Technology companies favor federal privacy legislation for the same reason this Comment argues that it has become necessary – state privacy laws are on the rise and complying with the different requirements of each will prove to be a difficult, if not an impossible task.[205]

Because of its national scope, a federal biometric privacy law would face more intense lobbying than the CCPA. Thus, Congress should attempt to balance the interests of technology companies, the data security industry, and individuals. The proper balance would be struck by excluding a private right of action and taking a tough stance on misuse, or even inadvertent disclosure of improperly stored or inadequately protected biometric information.

D. What Should Federal Biometric Privacy Legislation Include?

On August 3, 2020, Senators Jeff Merkley and Bernie Sanders introduced the National Biometric Information Privacy Act of 2020 (NBIPA).[206] While the introduction of this bill certainly adds support to the push for federal biometric privacy legislation, this bill does not reflect the type of balanced and focused legislation urged by this Comment and seems unlikely to pass.[207] This section takes an in-depth look at NBIPA's flaws and suggests what a more balanced piece of federal biometric privacy legislation should look like.

1. An Overview of NBIPA

NBIPA defines "biometric identifier" as "a retina or iris scan; a voiceprint; a faceprint (including any faceprint derived from a photograph); fingerprints or palm prints; and any other uniquely identifying information based on the characteristics of an individual's gait or other immutable characteristics of an individual."[208] The definition excludes the following: "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or

[205] *Id.*
[206] N.Y. GEN. BUS. LAW § 899-bb.
[207] *Id.*
[208] *Id.*

physical descriptions such as height, weight, hair color, or eye color."[209] It also excludes tissues associated with organ donation and health care information.[210]

The proposed legislation "limits the ability of companies to collect, buy, sell, lease, trade, or retain individuals' biometric information without specific written consent, and requires private companies to disclose to any inquiring individual the information the company has collected for that individual."[211] It contains both a private right of action and allows State Attorneys General to sue companies for violations.[212] While NBIPA is seemingly motivated by genuine concerns,[213] it ignores the broader purpose that such legislation would serve: to provide national regulations that businesses can bring themselves into alignment with and to remedy violations without overwhelming the courts with the likes of post-BIPA litigation.

---

[209] *Id.*

[210] *Id.*

[211] *See also* Press Release, Office of Senator Jeff Merkley, *Merkley, Sanders introduce legislation to put strict limits on corporate use of facial recognition* (Aug, 4, 2020), https://www.merkley.senate.gov/news/press-releases/merkley-sanders-introduce-legislation-to-put-strict-limits-on-corporate-use-of-facial-recognition-2020.

[212] *Id.*

[213] *Id.* Senator Merkley's website discussing NBIPA cites a 2019 study reporting "that Asian and Black individuals were up to 100 times more likely to be misidentified by facial recognition technology, signaling alarming consequences for the use of the technology to surveil stores." However, federal legislation seeking to regulate the collection and retention of biometric information by private entities should seek to protect that information in case of a breach or intentional misuse (i.e. selling biometric information for a profit without consent or legitimate purpose). The concerns addressed on Senator Merkley's website appear better suited for another piece of legislation dealing with the potential criminal implications of misidentification by facial recognition software. The author of this Comment is aware that Senator Merkley also helped introduce the "Facial Recognition and Biometric Technology Moratorium Act" and the "Ethical Use of Facial Recognition Act," both of which seem far more suited for the purpose stated on Senator Merkley's NBIPA website.

2. Proposed Contents of Federal Biometric Privacy Legislation

Although NBIPA represents a good first attempt, this Comment argues that it does not strike the proper balance between individuals' privacy rights and the needs of businesses operating in a world that has become increasingly reliant on biometrics. First, a federal law governing biometric privacy must include a comprehensive definition of biometrics. While it is obvious that this definition should be as comprehensive as possible, biometrics' constantly evolving nature will doubtlessly make it impossible to be exhaustive.[214] The state laws discussed in Section II and NBIPA each define biometrics in slightly different ways.[215] Despite these differences, each includes fingerprints, voiceprints, and scans of retinas or irises.[216] Since these identifiers appear to be generally accepted, they should be included in the federal definition of biometrics.

In addition to these identifiers, federal legislation should also include scans of face or hand geometry. These identifiers were included in NBIPA and the Illinois and Texas statutes.[217] While the inclusion of these biometric identifiers may have spurred some of the post-BIPA class action litigation, this would not be an issue in federal legislation that excludes a private right of action. The inclusion of scanned face and hand geometry in the definition of biometric identifiers will help protect additional sensitive privacy rights of

[214] Benson, *supra* note 156, at 188.
[215] 740 ILL. COMP. STAT. ANN. 14/10 (West 2021); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021); WASH. REV. CODE ANN. § 19.375.010 (West 2021).
[216] 740 ILL. COMP. STAT. ANN. 14/10 (West 2021); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021); WASH. REV. CODE ANN. § 19.375.010 (West 2021).
[217] 740 ILL. COMP. STAT. ANN. 14/10 (West 2021); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).

consumers.[218] If this information was mishandled or misused, it could be just as detrimental as the other commonly included identifiers.[219]

Second, to be effective, a federal biometric privacy law must contain regulations concerning the collection, storage, use, disclosure, and sale of biometric identifiers or information. State biometric privacy laws and NBIPA vary in how they approach these regulations.[220] However, as with the definition of biometrics, there exists some general consensus. Each statute requires notice and consent for collection, reasonable security measures for storage, and restrictions on disclosure, retention, and destruction.[221] In regards to disclosure, the state statutes permit biometric identifiers or information to be disclosed when (1) consented to; (2) required by law; (3) pursuant to a warrant,[222] subpoena,[223] or court order;[224] or (4) necessary to complete authorized financial transactions.[225] The federal legislation should adopt each of these agreed upon features.

On the subject of the sale of biometric data, the statutes vary. For example, BIPA prohibits the sale of biometric identifiers,[226] Texas allows biometric data sale under a limited set of circumstances,[227] Washington allows sale more broadly while still limiting and enumerating when it is allowed,[228] and NBIPA's language also seems

[218] Steve Symanovich, *How Does Facial Recognition Work?*, NORTON, https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html.
[219] *Id.* ("Your facial data can be collected and stored, often without your permission. It's possible hackers could access and steal that data.").
[220] Tumeh, *supra* note 59.
[221] *Id.* (noting, however, that Illinois is the only state which clearly defines what its notice and consent requirements are).
[222] *Id.* (noting that Illinois and Texas include disclosure pursuant to a warrant).
[223] *Id.* (noting that Washington permits disclosure pursuant to a court order).
[224] *Id.* (noting that Illinois permits disclosure pursuant to a subpoena).
[225] *Id.*
[226] 740 ILL. COMP. STAT. ANN. 14/15 (West 2021) (stating in relevant part that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.").
[227] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021) (stating the conditions under which biometric identifiers captured for commercial purposes may be sold, leased, or disclosed).
[228] WASH. REV. CODE ANN. § 19.375.020 (West 2021).

to prohibit the sale of biometric identifiers.[229] The way the Washington and Texas statutes were drafted allows the sale of biometric identifiers when the disclosure requirements listed in the preceding paragraph are met.[230] Unlike BIPA, federal legislation should not impose an all-out ban on the sale of biometric identifiers or information. Rather, it should mirror Texas' and Washington's restricted sale framework.[231]

As discussed in Section II.E.3, Washington's statute includes several additional instances where disclosure – and, by extension, sale – would be permitted, these include when it: (1) adheres to the requisite notice, consent, security, and retention provisions; (2) is "necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual"; (3) is "made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent" provisions; (4) "is required or authorized by a federal or state statute, or court order"; or (5) is made in preparation for litigation or judicial process.[232]

This Comment proposes that Washington's approach to the sale of biometric identifiers should be adopted at the federal level wholly or at least in part. As mentioned previously, Washington permits the sale of biometric identifiers under stringent and limited circumstances.[233] Washington's extended list of acceptable terms for sale and disclosure appears to provide the best balance between individual and commercial interests.[234] While biometric identifiers may be disclosed under BIPA under certain circumstances, selling biometric identifiers is completely prohibited.[235] Businesses that wish to sell biometric information should be permitted to do so in limited

[229] *See* N.Y. GEN. BUS. LAW § 899-bb.
[230] Tumeh, *supra* note 59.
[231] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021); WASH. REV. CODE ANN. § 19.375.020 (West 2021).
[232] WASH. REV. CODE ANN. § 19.375.020 (West 2021); Tumeh, *supra* note 59.
[233] Tumeh, *supra* note 59.
[234] *Id.*
[235] *Id.*

circumstances, such as with permission or in order to accomplish something requested by the consumer. The total elimination of this option in BIPA is too restrictive and should not be replicated at the federal level. At the very least, Congress should be no more restrictive than the Texas statute – allowing the sale of identifiers per a more limited list of disclosure exceptions.[236]

Third, the federal legislation should be limited in scope to commercial purposes. The Texas and Washington statutes are both limited in such a way; however, only Washington's statute defines that term.[237] Washington defines commercial purpose as "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."[238] The requirement of a different or unrelated purpose is crucial to this definition and how the Washington statute functions. This type of use triggers the other requirements like notice and consent, security measures, and restrictions on sale, disclosure, retention, and destruction.

It is also worth noting that Washington's definition of commercial purpose excludes law enforcement or security purposes.[239] In contrast, BIPA contains neither a commercial purpose limitation, nor an exception for security purposes from its definition; these continue to be two major contributors to the post-enactment BIPA litigation. Some of the most contentious cases following the enactment of BIPA stemmed from employees dissatisfied with the use of biometrics for security or identity verification purposes.[240] In fact,

[236] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).
[237] Tumeh, *supra* note 59.
[238] WASH. REV. CODE ANN. § 19.375.010 (West 2021).
[239] *Id.*
[240] Winter et al., *supra* note 102.

BIPA contains language indicating that it was enacted as a reaction to increased reliance on biometrics in "security screenings."[241]

Federal legislation should include a definition of commercial purpose and carve out an exception for security and law enforcement purposes. In terms of defining commercial purpose, the use of biometric identifiers for purposes unrelated to the original collection seem to amass the majority of individual privacy concerns. An unrelated purpose also seems to implicate a certain level of misuse which is ultimately what the federal legislation should aim to target.

Fourth, for the reasons outlined in Section III.C,[242] federal legislation should contain a section assigning enforcement powers to the states' attorneys general. The legislation should also expressly state that it does not create a private right of action.[243]

Lastly, the legislation must contain penalties for violations. On this particular subject, the state statutes vary widely. While proposing a specific figure for violations would be beyond the scope of this Comment, the adoption of a distinction between 'violation' and 'intentional violation' seems reasonable. Intentional violations of the federal legislation should be subject to a heftier penalty than inadvertent or even reckless violations. This ties back to the idea that the federal legislation should be focused on some type of misuse, rather than the mere implication of privacy interests.

---

[241] 740 ILL. COMP. STAT. ANN. 14/5 (West 2021) (stating "The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.").

[242] *See* discussion *supra* Section III.C.

[243] 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. U. Chi. L.J. 117, 139 (2017) (Courts have used judicial power to create implied private rights of action in certain scenarios, however "[a] plaintiff seeking to imply a private action today has the burden of proof to overcome the presumption against the judicial creation of new implied actions." By including a statement expressly excluding a private right of action, this presumption against the judicial creation will be much stronger.).

With the inclusion of face and hand geometry, the exclusion of a private right of action, a definition of commercial purpose, carve outs for security and law enforcement purposes, and a misuse requirement, the federal legislation will be in excellent shape to protect individual privacy rights and the interests of businesses that use biometric information in their operations. This construction allows states' attorneys general to pursue cases in which privacy rights have truly been violated and will prevent the excessive and burdensome litigation seen after BIPA was enacted.

IV. CONCLUSION

In sum, the United States needs federal biometric privacy legislation for two reasons: first, to protect individual biometric privacy on a national level, and second, to provide uniform guidelines to which businesses can conform their practices. The current patchwork system in place is inadequate to provide consumers the protection they deserve, and the rise of state legislation on the subject of biometric privacy is injurious to businesses operating nationally.

Federal legislation must strike a careful balance between the concern for individual privacy rights and the legitimate reasons businesses have started to use biometric identifiers in the private sector. State laws on the subject provide some helpful insight for the construction of this federal legislation; however, this Comment would caution against using BIPA as the model for three reasons. First, BIPA is unnecessarily restrictive on businesses because it bans the sale of biometric information for any reason. Second, BIPA created a private right of action that continues to be a source of numerous class action lawsuits. Lastly, BIPA failed to provide any carve outs for security or law enforcement purposes, which is another contributing factor to the extensive litigation.

This Comment argues that these three issues would be untenable at the national level. A strict prohibition on the sale of biometric information would result in intensive lobbying against the legislation and its ultimate defeat. Creating a private right of action and failing to provide carve outs for security and law enforcement would overburden the court systems. Additionally, there is no reason

why states' attorneys general may not competently bring the claims under the federal legislation. Unfortunately, the current proposed federal biometric privacy legislation, NBIPA, seems more similar to BIPA than to Texas' or Washington's statutes; this may contribute to what this author expects to be its ultimate failure.

To achieve the balance necessary for a federal biometric privacy law, the legislation should include: (1) a definition of biometric identifiers that includes fingerprints, voiceprints, scans of retinas or irises, and face or hand geometry; (2) a definition of 'commercial purpose' that limits the scope of the legislation; (3) exemptions for security and law enforcement purposes; (4) an express statement that no private right of action exists; (5) an assignment of enforcement powers to the states' attorneys general; (6) a misuse requirement and appropriate penalties for different levels of violations; (7) permissible disclosure when: consented to, required by law, pursuant to a warrant, subpoena, or court order, or necessary to complete authorized financial transactions; and (8) the limited instances in which sale of the biometric identifiers is permitted under Washington's statute.

The suggested inclusions and exclusions above would limit litigation to cases in which rights have genuinely been violated and sensitive data exposed, either inadvertently or in direct violation of the law. These provisions would prevent the stifling of industry and stand a good chance of gaining support from both sides of the aisle – garnering support from consumer-focused and business-focused advocates alike. These propositions would provide the best balance and secure the nationwide biometric privacy legislation this country needs.