Brooklyn Law Review

Volume 86 | Issue 3 Article 9

12-1-2021

Putting a Finger on Biometric Privacy Laws: How Congress Can Stitch Together the Patchwork of Biometric Privacy Laws in the United States

Eliza Simons

Putting a Finger on Biometric Privacy Laws

HOW CONGRESS CAN STITCH TOGETHER THE PATCHWORK OF BIOMETRIC PRIVACY LAWS IN THE UNITED STATES

Imagine this: You are waiting in line to pay at a store. You are called to the register, the cashier rings you up and you reach for your wallet to pull out your credit card, but it's not there. Panic sets in as you realize it was stolen. You consult your bank statements for any unauthorized charges. Luckily, there are only a few insignificant purchases. Not to despair, you call your bank, cancel your card, and are issued a new credit card with an entirely new number.[1] Your bank account is safe. Crisis averted.

Now, imagine this: It's twenty years into the future. You are, again, waiting in line to pay at the same store, except now, stores only accept payment through fingerprint identification. You think nothing of it, as you recognize the convenience of, quite literally, always having your method of payment right at your fingertips. You are called to the register, the cashier rings you up, and you touch your finger to a sensor to authorize the transaction.[2] The cashier informs you that your bank account is empty. You check your phone only to see a notification from a store where you recently shopped: "Data Breach." You remember back to when you made the purchase, you were asked to give your fingerprint to authenticate the transaction. You quickly connect the dots and realize your fingerprint has fallen into the hands of a hacker. What now?

---

[1] *Report Lost or Stolen Card*, DISCOVER, https://www.discover.com/credit-cards/help-center/faqs/lost-stolen.html [https://perma.cc/588W-FA6X].

[2] *Fingerprint Authentication Moves from Phones to Payment Cards*, VISA, https://usa.visa.com/visa-everywhere/security/biometric-payment-card.html [https://perma.cc/D3QU-6Y7Q].

INTRODUCTION

Your fingerprint is a biometric identifier, defined as a "unique physical characteristic."[3] Broken down, the root word "bio" refers to life[4] and the root word "metric" refers to a measurement.[5] Thus, "biometrics" refers to a way to identify humans based on their unique biological and behavioral characteristics.[6] Fingerprints are the most common among biometric identifiers,[7] but others include your eye scan, voiceprint, facial geometry, palm and vein patterns, and heartbeat patterns.[8] Sources suggest that biometric identifiers may also include the way you sit, the way you walk, your body odor, and possibly your eye blinking patterns.[9] Given its unique and irreplaceable nature, once biometric information falls into the wrong hands, there is no redress.[10] This risk emphasizes the importance of protecting biometric information and with that, an individual's desire to keep this information private.[11]

The distinctive nature of biometric identification is why both public and private entities have incorporated biometric technology as a means of security, convenience, and cost cutting.[12]

---

[3] *Biometrics*, DEP'T HOMELAND SECURITY (July 9, 2021), https://www.dhs.gov/biometrics [https://perma.cc/A3T9-NKA7].

[4] *Bio*, DICTIONARY.COM, https://www.dictionary.com/browse/bio?s=t [https://perma.cc/Q859-LHPC].

[5] *Metric*, DICTIONARY.COM, https://www.dictionary.com/browse/metric?s=t [https://perma.cc/T9VB-JWND].

[6] *What is Biometrics Security*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/biometrics [https://perma.cc/67GS-WSE7].

[7] RACHEL GERMAN & K. SUZANNE BARBER, UNIV. OF TEX. CTR. FOR IDENTITY, CURRENT BIOMETRIC ADOPTION AND TRENDS 2 (Sept. 2017), https://identity.utexas.edu/sites/default/files/2020-09/Current%20Biometric%20Adoption%20and%20Trends.pdf [https://perma.cc/7GJ5-XUDY].

[8] *See* 740 ILL. COMP. STAT. 14/10; WASH. REV. CODE § 19.375.020; TEX. BUS. & COM. CODE ANN. § 503.001; GERMAN & BARBER, *supra* note 7. The Illinois Biometric Information Privacy Act (BIPA) clarifies that biometric information does not include physical descriptions, donated organs or tissues, biological materials, photographs, or written signatures. *See* 740 ILL. COMP. STAT. 14/10.

[9] *See What Is Biometrics Security*, *supra* note 6; Sherif N. Abbas Seha & M. Abo-Zahhad, *Eye Blinking EOG Signals as Biometrics*, *in* BIOMETRIC SECURITY AND PRIVACY: OPPORTUNITIES & CHALLENGES IN THE BIG DATA ERA 121–22 (Richard Jiang et al. eds. 2017).

[10] 740 ILL. COMP. STAT. 14/5 ("Biometric . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse.").

[11] *See* RACHEL L. GERMAN & K. SUZANNE BARBER, UNIV. OF TEX. CTR. FOR IDENTITY, CONSUMER ATTITUDES ABOUT BIOMETRIC INFORMATION 15 (May 2018), https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf [https://perma.cc/T4W8-ZASK] (showing that the prevailing reason why survey respondents were not comfortable with biometric identification was because of a concern of invasion of privacy).

[12] *See generally* GOODBYE, PASSWORDS. HELLO BIOMETRICS, VISA, https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-biometrics-payments-study.pdf [https://perma.cc/N2BG-5GJ6]; Selena Larson, *Beyond Passwords: Fingerprints and Digital Behavior to ID Employees*, CNN BUS. (Mar. 18, 2018, 3:53 PM), https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html [https://perma.cc/69YS-EJCG]; Lauren Lowrey, *Biometric Payments Expanding to Grocery and Convenience Stores*,

Because of these benefits, it has become increasingly common to using biometric data to authenticate a transaction or verify information.[13] Biometric data usage is expanding even further amidst the COVID-19 pandemic as a way to maintain social distancing.[14] In 2018, sixty two percent of companies used some form of biometric authentication technology[15] and the global biometric market was worth $17.28 billion.[16] In 2020, the global biometrics market was valuated at $23.5 billion. By 2022, the mobile biometrics market is expected to be worth $49.33 billion[17] and $68.6 billion by 2025.[18] In the United States, the fingerprint sensor market alone is projected to reach $7.1 billion by 2024.[19] Despite the economic effects of the COVID-19 pandemic, the global biometrics market is forecasted to be worth at least $82 billion by 2027.[20] Eventually, to authenticate a transaction or identify yourself, you will be asked to provide "something that you are, rather than something that you know."[21]

SECUREID NEWS, (Feb. 2, 2005), https://www.secureidnews.com/news-item/biometric-payments-expanding-to-grocery-and-convenience-stores/ [https://perma.cc/3YYM-LM5Q].

[13] *See* GERMAN & BARBER, *supra* note 7.

[14] David Oberly, *Biometric Data and COVID-19 in The Workplace*, JD SUPRA (Nov. 23, 2020), https://www.jdsupra.com/legalnews/biometric-data-and-covid-19-in-the-86112/ [https://perma.cc/2JJL-V638].

[15] *See* Peter Tsai, *Data Snapshot: Biometrics in the Workplace Commonplace, But are They Secure?*, SPICEWORKS (Mar. 12, 2018), https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure [https://perma.cc/ED8Y-DMYT].

[16] *Global Biometrics Industry Report 2020: Set to Reach $76.6 Billion by 2027 – Includes an Assessment of the Coronavirus' Impact on the Industry*, INTRADO GLOBAL NEWSWIRE (Apr. 27, 2020, 6:08 AM), https://www.globenewswire.com/news-release/2020/04/27/2022258/0/en/Global-Biometrics-Industry-Report-2020-Set-to-Reach-76-6-Billion-by-2027-Includes-an-Assessment-of-the-Coronavirus-Impact-on-the-Industry.html#:~:text=The%20Global%20Biometrics%20market%20accounted,18%25%20during%20the%20forecast%20period [https://perma.cc/V476-RYPL].

[17] *Mobile Biometrics Market worth 49.33 Billion USD by 2022*, MARKETS & MARKETS (Aug. 2016), https://www.marketsandmarkets.com/PressReleases/mobile-biometric.asp [https://perma.cc/LJ6H-8Y8K].

[18] *Biometric System Market Worth $68.6 Billion by 2025*, MARKETS & MARKETS (Nov. 11, 2020), https://www.marketsandmarkets.com/PressReleases/biometric-technologies.asp [https://perma.cc/K7JS-T8HU].

[19] *Fingerprint Sensor Market by Technology (Capacitive, Optical, Thermal, Ultrasonic), Type (Touchy, Swipe,), Application (Consumer Electronics, Banking & Finance, Government & Law Enforcement, Commercial, Smart Homes), and Region-Global Forecast to 2024*, MARKETS & MARKETS (Sept. 2019), https://www.marketsandmarkets.com/Market-Reports/fingerprint-sensors-market-169519533.html [https://perma.cc/5JYJ-LXGG].

[20] Chris Burt, *Global Biometrics Market Forecast to Surpass $82B by 2027 Despite Pandemic*, BIOMETRIC UPDATE (Oct. 14, 2020), https://www.biometricupdate.com/202010/global-biometrics-market-forecast-to-surpass-82b-by-2027-despite-pandemic [https://perma.cc/8D7C-CME3].

[21] Kaveh Waddell, *When Fingerprints are as Easy to Steal as Passwords*, ATLANTIC (Mar. 24, 2017), https://www.theatlantic.com/technology/archive/2017/03/new-biometrics/520695/ [https://perma.cc/N8YA-SQ8K]; Bruce Schneier, *Stealing Fingerprints*, VICE (Sept. 29, 2015, 11:25 AM), https://www.vice.com/en_us/article/78x5va/stealing-fingerprints [https://perma.cc/5LMQ-6C5H].

The level of protection provided by biometric identification far surpasses that of passwords and PIN numbers.[22] The tradeoff for these security benefits, however, is the risk of a data breach and the dangerous reality that unlike your credit card, social security number, and driver's license, you cannot simply be issued a new fingerprint.[23] There are several consequences of a biometric data breach and some have yet to be realized.[24] So far, it has been reported that hackers can replicate a fingerprint to break into a security system.[25] This was proven in 2014 when a hacker recreated a German minister's fingerprints using only a photo of the minister's hands.[26] Jason Chaikin, the president of a biometrics company, confirmed this when he unlocked an iPhone using a fingerprint imprinted into Play-Doh.[27] Chaikin performed this demonstration to his company to demonstrate how vulnerable our fingerprints

---

[22] *See* Louis Columbus, *Why Your Biometrics Are Your Best Password*, FORBES (Mar. 8, 2020, 12:38 PM), https://www.forbes.com/sites/louiscolumbus/2020/03/08/why-your-biometrics-are-your-best-password/?sh=35fcca666c01 [https://perma.cc/QG2W-F726] (explaining that the security industry has tried to "kill the password for decades" because "81% of data breached involve weak, stolen, default, or otherwise compromised credentials"); John Trader, *How Effective are Biometrics as an Alternative to Passwords*, M2SYS BLOG (May 18, 2015), https://www.m2sys.com/blog/single-sign-on-sso/how-effective-are-biometrics-as-an-alternative-to-passwords/ [https://perma.cc/86N5-SZ2N] (explaining that the main cause of data breaches can be attributed to stolen passwords prompting companies to explore biometric technology). *But see* Jake Stroup, *Biometric Identification and Identity Theft*, THE BALANCE (Mar. 28, 2021), https://www.thebalance.com/biometric-identification-and-identity-theft-1947595 [https://perma.cc/T8RH-Y2B2] ("If we implement biometrics without doing our due diligence on protecting the identity, we are doomed to repeat history—and our thumbprint will become just another Social Security number."); Robinson Meyer, *Who Owns Your Face?*, ATLANTIC (July 2, 2015), https://www.theatlantic.com/technology/archive/2015/07/how-good-facial-recognition-technology-government-regulation/397289/ [https://perma.cc/V6EY-XAR4] (suggesting that facial identification is less secure *because* it cannot be changed).

[23] *See* Stroup, *supra* note 22; *Can I Change My Social Security Number?*, SOC. SECURITY ADMIN. (Nov. 30, 2019), https://faq.ssa.gov/en-US/Topic/article/KA-02220 [https://perma.cc/6GJX-QMJ5]; *Frequently Asked Questions, What do I do if my Credit Card is Lost or Stolen?*, CHASE, https://www.chase.com/personal/credit-cards/card-resource-center/cardreplace#_cardrpl-2 [https://perma.cc/P36D-684D]; *How to Replace a License or Permit*, N.Y. ST. DEP'T MOTOR VEHICLES, https://dmv.ny.gov/driver-license/how-replace-license-or-permit [https://perma.cc/C8MA-KW6R]; Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, FORBES (Aug. 14, 2019, 4:31 AM), https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=5659dc9e46c6 [https://perma.cc/VA8E-NBHW]; NIYA T. MCCRAY, FOR THE DEFENSE, THE EVOLUTION OF U.S. BIOMETRIC PRIVACY LAW 78 (May 2018), https://www.bradley.com/-/media/files/insights/publications/2018/05/ftd1805mccray.pdf [https://perma.cc/N5QE-TM93].

[24] *See* MCCRAY, *supra* note 23, at 77.

[25] Aaron Mak, *What Can a Hacker Do With Your Stolen Fingerprints?*, SLATE (Aug. 15, 2019, 5:52 PM), https://slate.com/technology/2019/08/how-criminals-might-use-stolen-fingerprints.html [https://perma.cc/7V62-5U7W].

[26] Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, GUARDIAN (Dec. 30, 2014, 6:43 AM), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands [https://perma.cc/43UB-49ZV].

[27] Jeff John Roberts, *This Guy Unlocked My iPhone With Play-Doh*, FORTUNE (Apr. 7, 2016, 11:55 AM), https://fortune.com/2016/04/07/guy-unlocked-iphone-play-doh/ [https://perma.cc/3KDA-9BHA].

actually are, and perhaps, that they are not as secure as consumers think.[28] Cryptographer Tsutomu Matsumoto was able to trick a fingerprint sensor using a gummy bear.[29] It has also been suggested that iris scans can be recreated to deceive iris-recognition software.[30] Perhaps even more troubling is the unpredictability of what a hacker can do with stolen facial recognition.[31] Researchers from a company specializing in artificial intelligence recently developed 3D masks depicting other people's facial features, which fooled airport facial recognition devices into believing the researchers were someone they were not.[32] These hacks illustrate that biometric authentication may not be as foolproof as one would like to believe.

This note argues that current legislation is insufficient to address the problems posed by the increased use of biometric data in the private sector. Because biometric identifiers are irreplaceable, their increased use in the private sector creates a need for a federal law that specifically regulates biometric data collection and usage. Although most states have general privacy laws, very few specifically regulate biometric privacy. Further, the few states that have enacted biometric privacy-specific laws face problems enforcing these laws. Challenges to defining biometric identifiers and debates about Article III constitutional standing have made state biometric privacy laws controversial. To address these problems, Congress should enact a federal law that considers both consumer privacy and secure and cost-effective business practices. The federal law should include a broad definition of biometric identifier, adopt consumer protections modeled after the rights granted to consumers in the California Consumer Privacy Act (CCPA), and consider an enforcement mechanism to best protect against the risks associated with collecting biometric information.

Part I of this note outlines the proliferation of biometric data collection in the private sector to underscore the need for biometric privacy regulation. It then describes the current legal framework of privacy law in both state and federal government, surveying privacy law based on four categories: (1) general federal privacy laws; (2)

---

[28] *Id.*

[29] John Leyden, *Gummi Bears Defeat Fingerprint Sensors*, REGISTER (May 16, 2002, 12:35 PM), https://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/ [https://perma.cc/NG2D-P6RJ].

[30] Kim Zetter, *Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners*, WIRED (July 25, 2012, 6:00 AM), https://www.wired.com/2012/07/reverse-engineering-iris-scans/ [https://perma.cc/2NXQ-RXZE].

[31] *See* Mak, *supra* note 25.

[32] Fabienne Lang, *Facial Masks Fool Airport Facial Recognition Technology, Researchers Discovered*, INTERESTING ENGINEERING (Dec. 16, 2019), https://interestingengineering.com/printed-masks-fool-airport-facial-recognition-technology-researchers-discovered [https://perma.cc/BSJ8-E8FQ].

general state privacy laws, (3) state biometric privacy laws, and (4) a federal biometric privacy law, or lack thereof. Part II looks at the issues with Illinois' Biometric Information Privacy Act, the strictest state biometric privacy law, and the ways these issues could be used to shape a federal biometric privacy law. Finally, Part III calls on Congress to protect biometric information of consumers in all fifty states through federal legislation. Ultimately, as this note proposes, a successful federal law will both guard against the risks associated with collection and use of consumer biometric data, but will also consider the cost, security, and convenience benefits of using biometric information in the private sector.

I. BACKGROUND

As biometric data collection becomes more prevalent,[33] naturally, a primary concern is the possibility of personal information falling into the wrong hands.[34] The number of data breaches in recent years[35] might explain the feeling of skepticism and distrust among Americans whose biometric information has been collected.[36] Though federal government agencies that collect personal information must comply with the Privacy Act,[37] the question remains how consumers will hold private entities accountable when they fail to protect our unique biometric data.

A. The Age of Biometrics: Rise of Biometrics in the Private Sector

We have recently entered an era where passwords and PIN codes have become secondary to other security measures.[38] In the public sector, biometric data is used at airports by the Department of Homeland Security,[39] as well as public employers

---

[33] *See* Tsai, *supra* note 15.

[34] *See* GERMAN & BARBER, *supra* note 11, at 2, 15; GOODBYE, PASSWORDS. HELLO BIOMETRICS, *supra* note 12.

[35] The Identity Theft Resource Center reported that in 2020, there were 1,108 data breaches across all industries in the United States, impacting 300,562,519 individuals. *Identity Theft Resource Center's 2020 Annual Data Breach Report Reveals 19 Percent Decrease in Breaches*, IDENTITY THEFT RESOURCE CTR. (Jan. 28, 2021), https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/ [https://perma.cc/S29N-M96S].

[36] According to a study done by the University of Texas, 86 percent of respondents were concerned about their personal information being misused. *See* GERMAN & BARBER, *supra* note 11, at 24. *But see Banking on Biometrics: Half of Cardholders Would Switch*, VISA (Jan. 2, 2020, 6:30 PM), https://usa.visa.com/visa-everywhere/blog/bdp/2020/01/02/banking-on-biometrics-1578003687083.html [https://perma.cc/6H3A-5BFH] (reporting that 53 percent of cardholders would switch banks if their bank did not offer biometric authentication).

[37] 5 U.S.C. § 552a.

[38] *See* Larson, *supra* note 12; MCCRAY, *supra* note 23.

[39] *See Biometrics*, *supra* note 3.

like the Department of Defense[40] and by the FBI.[41] For example, Delta Airlines recently partnered with Customs and Border Patrol to create a self-boarding gate that uses facial recognition to verify travelers' identities.[42] The surge in biometric data usage, however, is seen largely in the private sector, where it is used for workforce management, banking, healthcare, and retail.[43] Large employers now require employees to provide biometric identifiers for time-clocking, unlocking doors and accessing laptops and tablets.[44] Employers also use biometric scanners to more efficiently track their employees' hours and eliminate the costs associated with "buddy punching."[45]

Most commonly, biometric identifiers have become popular in the consumer devices industry.[46] In 2013, Apple launched Touch ID, a feature that allows users to unlock their phones using their fingerprint.[47] A few years later, Apple replaced Touch ID with Face ID, which enables users to unlock their phones using their facial geometry, and which can even respond to changes in their physical appearance.[48] Additionally, in supermarkets and other brick-and-

---

[40] Kyle Rempfer, *Facial Recognition May be Coming to the Gate of an Air Force Base Near You*, AIRFORCETIMES (Mar. 1, 2019), https://www.airforcetimes.com/news/your-air-force/2019/03/01/facial-recognition-may-be-coming-to-the-gate-of-an-air-force-base-near-you/?utm_source=Sailthru&utm_medium=email&utm_campaign=Daily%203.6&utm_term=Editorial%20-%20Daily%20Brief [https://perma.cc/KFB3-W4SS].

[41] *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/D2WY-JHPG].

[42] Jessica Puckett, *How to Opt Out of Facial Recognition at the Airport*, CONDE NAST TRAVELER (Jan. 5, 2021), https://www.cntraveler.com/story/how-to-opt-out-of-facial-recognition-at-the-airport [https://perma.cc/Z7Q2-SCRN].

[43] Alan S. Wernick, *Biometric Information –Permanent Personally Identifiable Information Risk*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/ [https://perma.cc/D493-F49F].

[44] SUSAN GROSS SHOLINKSY & BARBARA HARRIS, EBG LAW, BIOMETRICS IN THE WORKPLACE 37 (June 2018), https://www.ebglaw.com/content/uploads/2018/06/PLJ-Jun18-Sholinsky-Feature-Biometrics-In-The-Workplace.pdf [https://perma.cc/W48E-WECJ]; *see* Tsai, *supra* note 15.

[45] *See* SHOLINSKY & HARRIS, *supra* note 44; "Buddy punching" is the practice of one employee recording the start time on another's employee's behalf before that employee has arrived at work. This practice results in employees getting paid for hours they have not worked. Danny Thakkar, *How Biometrics Can Cut Down Buddy Punching and Boost Operational Efficiency*, BAYOMETRIC, https://www.bayometric.com/biometrics-can-cut-buddy-punching/ [https://perma.cc/A294-2S43].

[46] PR Newswire, *Biometric Technologies Market to 2027 – Global Analysis and Forecasts by Retail Type; Shopping Type; Carrier Type*, MKTS. INSIDER (Sept. 18, 2019, 12:40 PM), https://markets.businessinsider.com/news/stocks/biometrics-technologies-market-to-2027-global-analysis-and-forecasts-by-retail-type-shopping-type-carrier-type-1028535148 [https://perma.cc/UR5U-ZK2W] ("The consumer devices industry is witnessing immense growth . . . majorly due to advancements and smart features.").

[47] Seth Rosenblatt, *iPhone 5S comes with Touch ID Fingerprint Scanner*, CNET (Sept. 10, 2013, 11:04 AM), http://news.cnet.com/8301-13579_3-57602245-37/fingerprint-sensor-touch-id-unlocks-new-iphones [https://perma.cc/T6QU-JWU4].

[48] *The Future is Here*: *iPhoneX*, APPLE: NEWSROOM (Sept. 12, 2017), https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x/ [https://perma.cc/PM82-

mortar retail stores, customers are able to complete transactions using biometric identifiers, such as fingerprint and facial recognition technology.[49] In 2016, Mastercard developed "selfie pay," technology whereby consumers pay by taking a photo of themselves.[50] Our world is rapidly transforming into one where a person's unique characteristics hold the key to completing everyday tasks. Given the acceleration of biometric data usage across the public, private, and consumer sectors, the time is ripe for federal regulation of biometric data. Yet, Congress has so far failed to take action to regulate the use of this advancement in technology. The bulk of current regulation has been enacted by states acting within their police power, leading to regulatory disarray, that creates an ineffective biometric data regulation regime.

B. The Current Legal Landscape: The Four Categories of Privacy Laws

Because of how our legal system values privacy, it is not surprising that a number of laws have come into play to regulate how our personal and biometric information is used.[51] When considering biometric privacy laws, the legal landscape of privacy law can be separated into four categories: (1) federal laws governing privacy generally; (2) state laws governing privacy generally; (3) state laws specifically regulating biometric privacy; (4) a federal law specifically governing biometric privacy. The fourth category is what is missing from the current regulatory

---

9DHM] (explaining that "Face ID projects more than 30,000 invisible IR dots" which are "pushed through neural networks to create a mathematical model of your face").

[49] *See* Lowrey, *supra* note 12; Sam Dean, *Forget Credit Cards – Now You Can Pay With Your Face. Creepy or Cool?*, L.A. TIMES (Aug. 14, 2020, 5:00 AM), https://www.latimes.com/business/technology/story/2020-08-14/facial-recognition-payment-technology [https://perma.cc/J5VX-WPJH].

[50] Alanna Petroff, *MasterCard Launching Selfie Payments*, CNN BUS. (Feb. 22, 2016, 1:43 PM), https://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/ [https://perma.cc/BGH3-SXUH].

[51] The right to privacy is highly valued in the United States: the Fourth Amendment guarantees the privacy of people and their possessions from unreasonable searches; Congress passed the Health Insurance Portability and Accountability Act, known as HIPAA, to protect personal information collected by healthcare providers; the Gramm-Leach-Bliley Act was passed to protect an individual's private financial information; and a line of Supreme Court cases have announced "zones of privacy" implicit in due process. U.S. CONST. amend. IV; 42 U.S.C. § 1320d-6; 15 U.S.C. § 6801; Lawrence v. Texas, 539 U.S. 558, 564–65 (2003); Planned Parenthood of Sw. Pa. v. Casey, 505 U.S. 833, 896 (1992); Roe v. Wade, 410 U.S. 113, 153 (1973) ("This right of privacy . . . is broad enough to encompass a woman's right to terminate her pregnancy."); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) ("If the right to privacy means anything, it is the right of the individual . . . to be free from unwarranted governmental intrusion."); Griswold v. Connecticut, 381 U.S. 479, 484 (1965) ("Various guarantees create zones of privacy."). In 1974, Congress passed The Privacy Act, which requires executive agencies to abide by rules for collection, retention, use, and disclosure when gathering an individual's personal records. 5 U.S.C. § 552a.

scheme. This section will give a brief overview of the first three categories. The next section will provide a framework for creating the fourth category by proposing solutions to problems created by state biometric privacy laws.

1. Federal Laws Governing Privacy Generally

Currently, there is no overarching federal law that governs data privacy. Instead, a patchwork of federal laws protects individual privacy from federal agencies and private entities in a way that has been called the "sectoral" or "industry-specific" approach.[52] In the public sector, federal laws regulate how federal agencies manage individuals' personal records.[53] These laws protect personal data collected by the Census Bureau,[54] state Departments of Motor Vehicles, and government agencies that store information electronically.[55] Through the Privacy Act of 1974, government agencies are required to release personal "records" upon request.[56] While the Privacy Act's definition of records does not explicitly include biometric identifiers, it does include fingerprints or voice prints.[57] Since passage of the Privacy Act in 1974, federal agencies have collected biometric data and the Act has been interpreted by some to include regulation of biometric data collection by federal agencies.[58] The Privacy Act is the primary statute regulating government-collected biometric data, but it is limited in scope as it applies to neither state and local governments nor private entities or businesses.

In the private sector, the Fair Credit Reporting Act requires consumer reporting agencies to adopt standards for

---

[52] Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 KAN. L. REV. 637, 644–45 (2018) ("[T]he United States has developed a sectoral approach, where data privacy protection is limited to specific types of information in limited circumstances."); 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) ("Although federal law in the United States is not entirely without data privacy regulation, regulations at the federal level are industry-specific.").

[53] 13 U.S.C. § 9; 44 U.S.C. §§ 3502, 3506 (E-Government Act of 2002).

[54] 13 U.S.C. § 9.

[55] 44 U.S.C. § 3502.

[56] 5 U.S.C. § 552a.

[57] 5 U.S.C. § 552a(a)(4). The Act defines record as "information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name . . . or other identifying particular assigned to the individual, such as finger or voice print or a photograph." *Id.*

[58] *See Biometrics*, *supra* note 3; *Next Generation Identification (NGI)*, *supra* note 41; Alexa N. Acquista, *Biometrics Takes Off—Fight Between Privacy and Aviation Security Wages On*, 85 J. AIR L. & COM. 475, 489–90 (2020) (identifying four main requirements the Privacy Act of 1974 imposes on federal agencies that collection biometric data).

protecting private consumer information contained in credit reports.[59] The Cable Communications Privacy Act requires cable providers and service operators to protect subscribers' privacy by providing written notice to subscribers in writing of "the nature of the personally identifiable information collected" and "shall not disclose personally identifiable information concerning any subscriber without . . . consent . . . and shall take such actions as are necessary to prevent unauthorized access to such information."[60] The Cable Act does not explicitly include biometric information in its definition of "personal identifiable information."[61]

Notably, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the only federal law to directly address biometric privacy.[62] HIPAA regulates privacy within the healthcare industry by prohibiting "covered entities"[63] from using or disclosing "protected health information"[64] to persons other than the protected individual or for reasons other than treatment and healthcare operations.[65] HIPAA grants individuals a "right to notice" as to the use and disclosure of that individual's information; a "[r]ight . . . request restriction of uses and disclosures" of protected health information; and a "right of access to inspect and obtain a copy of protected health information."[66] If an individual finds any of that information to be incorrect, they have a "[r]ight to amend" their record.[67] Further, HIPAA requires covered entities to make "reasonable efforts to limit protected health information."[68] The U.S. Department of Health & Human Services' ("HHS") Office of Civil Rights is the agency tasked with HIPAA enforcement by investigating complaints filed with the HHS, "conducting compliance reviews," and "performing education and outreach to foster compliance . . . ."[69] Finally, HIPAA does not

---

[59] 15 U.S.C. § 1681.

[60] 47 U.S.C. § 551.

[61] 47 U.S.C. § 551(a)(2)(A) ("[T]he term 'personally identifiable information' does not include any record of aggregate data which does not identify particular persons.").

[62] 45 C.F.R. § 164.514(b)(2)(i)(P).

[63] A covered entity is a "(1) health plan, (2) health clearing house[, or] (3) [a] health care provider who transmits any health information in electronic form in connection with a transaction." 45 C.F.R. § 160.103. This definition also includes "a business associate of another covered entity." *Id.*

[64] Protected health information is defined as "individually identifiable health information . . . that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium." *Id.*

[65] 45 C.F.R. § 164.502(a).

[66] 45 C.F.R. §§ 164.522, .524.

[67] 45 C.F.R. § 164.526.

[68] 45 C.F.R. § 164.502(b).

[69] *Enforcement Process*, U.S. DEP'T OF HEALTH & HUM. SERVS. (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html [https://perma.cc/2G69-AKPG].

create a private right of action,[70] which some have argued renders it a "toothless" privacy law that "does not properly incentivize covered entities to fully comply."[71]

2. State Laws Governing Privacy Generally

Although there are many state-level privacy laws that protect "personal information,"[72] few are specifically targeted at protecting "biometric information." Indeed, some state laws include biometric information in their definition of personal information,[73] but are not tailored to the unique nature of biometrics. For example, Maryland's Personal Information Protection Act, which also requires businesses to protect against "unauthorized access to personal information," includes biometric data in its definition of personal information.[74] In contrast, Utah's Protection of Personal Information Act provides that any business that maintains documentation of *personal information* is required to develop procedures that prevent unlawful disclosure and must promptly destroy personal information.[75] The statute's definition of "personal information" includes social security numbers, financial account numbers, security codes, and driver's license

---

[70] *See* Dodd v. Jones, 623 F.3d 563, 569 (8th Cir. 2010) (finding that plaintiff's HIPAA claim against a law enforcement officer in his individual capacity for unlawful search of his blood failed because "HIPAA does not create a private right of action"); *see also* Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006) ("Every district court that has considered [HIPAA enforcement] is in agreement that the statute does not support a private right of action.").

[71] Morgan Leigh Tendam, *The HIPAA-Pota-Mess: How HIPAA's Weak Enforcement Standards Have Led States to Create Confusing Medical Privacy Laws*, 79 OHIO ST. L.J. 411, 413, 421 (2018); Austin Rutherford, Byrne: *Closing the Gap Between HIPAA and Patient Privacy*, 53 SAN DIEGO L. REV. 201, 204 (2016) ("HIPAA's lack of individualized remedy harmed individualized and left the law a toothless monster."); Joshua D.W. Collins, *Toothless HIPAA: Searching For a Private Right of Action to Remedy Privacy Rule Regulations*, 60 VAND. L. REV. 199, 202–03 (2007).

[72] *See, e.g.*, MD. CODE ANN. § 10-1303 (requiring government agencies to consider four factors to prevent unauthorized access when destroying personal information); ARIZ. REV. STAT. ANN. § 18-552 (requiring businesses subject to a data breach notify the individuals whose personal information was collected and stored); KAN. STAT. ANN. § 75-7240 (requiring a government agency that maintains computerized data of personal information comply with data breach notification requirements); GA. CODE ANN. § 10-1-912 (Georgia's data security breach notification law); COLO. REV. STAT. ANN. § 14-5-712 (limiting state use of personal information in certain domestic relations matters).

[73] MD. CODE ANN. § 10-1301 ("Personal information means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image."); VT. CODE ANN. 8 § 2451 ("Personal information means data capable of being associated with a particular natural person, including gender identification, birth information, marital status, citizenship and nationality, biometric records."); COLO. REV. STAT. ANN. § 6-1-716 ("Personal information means a Colorado resident's first name . . . and last name in combinations with any one or more of the following . . . when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable . . . biometric data.").

[74] MD. CODE ANN. §§ 14-3503, -3501(e)(1).

[75] UTAH CODE ANN. § 13-44-201.

identification numbers.[76] The definition makes no mention of biometric information.[77]

A few states are moving towards an omnibus approach to data privacy.[78] In 2018, California was the first state to enact a general state privacy law.[79] In response to the Cambridge Analytica data scandal in March 2018,[80] which primarily impacted Californians,[81] the California legislature recognized the need to strengthen consumer privacy laws.[82] The legislature acknowledged that "the proliferation of personal information has limited Californians' ability to properly protect and safeguard their privacy" and subsequently passed the California Consumer Privacy Act (CCPA), aimed at giving consumers more control over who has access to their personal information.[83] The far-reaching CCPA impacts any private entity that does business in California or that collects or stores data about California residents. Given that many large companies do business nationwide, including in California, this legislation has the potential to set the standard for data collection throughout the country.

The CCPA defines both "personal information" and "biometric information."[84] The arguably broad definition of "personal information" includes, among other things, identifiers such as name, postal address, and social security number; commercial information including products or services purchase; Internet and electronic network activity information; geolocation data; professional and employment-related data; and most importantly for this discussion, biometric information. The CCPA's definition of biometric information encompasses "psychological, biological, or behavioral characteristics . . . that can be used . . . to establish individual

---

[76] UTAH CODE ANN. § 13-44-102(4).

[77] UTAH CODE ANN. § 13-44-201.

[78] S.B. 1392, 2021 Sess. (Va. 2021) (effective Jan. 1, 2023); S.B. 5062, 67th Leg., 2021 Reg. Sess. (Wash. 2021); S.B. 5642, 2019–2020 Reg. Sess. (N.Y. 2019); S.B. 418, 13th Leg. Sess. (Haw. 2019).

[79] CAL. CIV. CODE § 1798.100; Dimitri Sirota, *California's New Privacy Law Brings U.S. Closer to the GDPR*, TECHCRUNCH (Nov. 14, 2019, 2:55 P.M), https ://techcrunch.com/2019/11/14/californias-new-data-privacy-law-brings-u-s-closer-to-gdpr/ [https://perma.cc/5SM4-QUN8].

[80] In March 2018, Facebook exposed 87 million Facebook profiles to Cambridge Analytica, a data analytics company working on Donald Trump's presidential campaign, without users' permission. Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, VOX (May 2, 2018, 3:25 PM), htt ps://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica -trump-diagram [https://perma.cc/SAS3-XZ2N].

[81] Richard Nieva, *Most Facebook Users Hit by Cambridge Analytica Scandal are Californians*, CNET (June 13, 2018, 1:27 PM), https://www.cnet.com/news/most-facebook-users-hit-by-cambridge-analytica-scandal-are-californians/ [https://perma.cc/XVL6-BZTD].

[82] *See, e.g.*, Assemb. B. 375 (Cal. 2018).

[83] *Id.*

[84] CAL. CIV. CODE § 1798.140(c), (v).

identity."[85] The definition also contains a nonexhaustive list of examples that ranges from the classic biometric identifier—a fingerprint—to the less obvious example of gait patterns or rhythms.[86] The broad definition contemplates types of biometric identifiers not contemplated by other statutes, such as Illinois' Biometric Information Privacy Act.[87]

The CCPA grants consumers five rights to their personal information: the right to know, the right to access, the right to delete, the right to opt-out, and the right to nondiscrimination.[88] First, a consumer's "right to know" means that a business must inform consumers of the categories of personal information collected and the purpose for which it will be used.[89] While limited to collecting the information for that specified use, a business must inform the consumer if it wishes to use their personal information for a purpose not previously specified.[90] Second, a consumer's "right to access" allows them to request that a business that has collected their personal information to disclose the specific personal information that was collected.[91] Specifically, upon request from a consumer, a business must disclose:

> (1) [t]he categories of personal information it has collected about that consumer[;] (2) [t]he categories of sources from which the personal information is collected[;] (3) [t]he business or commercial purpose for collecting or selling personal information[;] (4) [t]he categories of third parties with whom the business shares personal information[; and] (5) [t]he specific pieces of personal information it has collected about that consumer.[92]

The business must promptly provide the required information to the consumer, free of charge.[93]

Third, the CCPA's "right to delete" allows consumers to request that the business dispose of any of their stored personal

---

[85] CAL. CIV. CODE § 1798.140.

[86] *Id.* ("'Biometric information' means an individual's physiological, biological or behavioral characteristics . . . . 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.").

[87] *See infra* Part I.B.3.a; *Is the CCPA's Definition of Biometric Information Broader than the Definition Used by Other States?*, BRYAN CAVE LEIGHTON PAISNER (Apr. 13, 2020), https://www.bclplaw.com/en-US/insights/is-the-ccpas-definition-of-biometric-information-broader-than-the-definition-used-by-other-states.html [https://perma.cc/XGD2-HDQX].

[88] CAL. CIV. CODE §§ 1798.100–.125.

[89] CAL. CIV. CODE § 1798.100(b).

[90] *Id.*

[91] CAL. CIV. CODE § 1798.100(a).

[92] CAL. CIV. CODE § 1798.110.

[93] CAL. CIV. CODE § 1798.100(d).

information.[94] Upon collection of the consumer's information, the business must inform the consumer of this right.[95] This right includes exceptions that allows businesses to refuse to comply with a customer's request. A business will not be required to comply with a consumer's request if retaining their information is necessary to accomplish any of the following: complete a requested transaction; "detect security incidents[,] identify and repair errors that impair" the business's functionality; "exercise free speech;" comply with California's Electronic Communications Privacy Act; engage in research that is in the public interest; enable a business's legitimate internal interests; and "comply with a legal obligation."[96]

The fourth right, the right to "opt-out," grants consumers the right to tell a business that it may not sell the consumer's personal information.[97] Like the right to delete, a business that sells consumers' personal information to third parties must inform consumers of this right.[98] Fifth, a consumer's "right to non-discrimination"[99] prevents a business from denying goods and services, charging "different prices or rates for good or services," or providing a different quality of goods or services in the event that a customer exercises the rights discussed above.[100] A business, however, may offer financial incentives to consumers in exchange for the collection of personal information, as long as the financial incentives are not "unjust, unreasonable, or usurious in nature."[101]

A notably unique feature of the CCPA is its two-dimensional method of enforcement. First, it grants consumers a limited private right of action.[102] Under this section,

> Any consumer whose nonencrypted and nonredacted personal information as defined in subparagraph (A) of paragraph (1) of subdivision (d) of [Cal. Civ. Code §] 1798.81.5, 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

---

94 CAL. CIV. CODE § 1798.105(a).

95 CAL. CIV. CODE § 1798.105(b).

96 *Id.*

97 CAL. CIV. CODE § 1798.120(a). This section does not apply to minors. A business is prohibited from selling personal information of consumers less than 16 years old if the business has actual knowledge of the consumer's age. CAL. CIV. CODE § 1798.120(c). Minor consumers have a "right to opt in" to the sale of their personal information. *Id.*

98 CAL. CIV. CODE § 1798.120(b).

99 CAL. CIV. CODE § 1798.125(a)(1).

100 *Id.*

101 CAL. CIV. CODE § 1798.125(b).

102 CAL. CIV. CODE § 1798.150.

> nature of the information to protect the personal information may institute a civil action.[103]

This right of action, however, is limited. It only applies to "nonencrypted and nonredacted personal information."[104] Therefore, companies can avoid individual suits by simply taking steps to encrypt personal information. Additionally, the limited private right of action has a narrower definition of personal information. Relevant to this discussion, this limited definition includes an individual's first name or initial and last name in combination with "[u]nique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual."[105] Another prerequisite to bringing an action under the CCPA is giving 30 days' written notice to the business "identifying the specific provisions of [the CCPA] the consumer alleges have been . . . violated" and affording the company an opportunity to cure the alleged violation.[106] Finally, a consumer can sue in their individual capacity if their biometric data is impacted by a data breach or is at risk of being impacted because a business failed to maintain reasonable security measures to protect the consumer's collected data.[107] Although, the CCPA does not define "reasonable security procedures," a related statue, the California's Reasonable Cybersecurity Statute, provides that "[a] business that . . . maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[108] Therefore, liability under the statute may hinge on whether a business can defend itself on the ground that it maintained "reasonable security procedures."

Given the novelty of the law, there has been little opportunity to test the efficacy of the CCPA's limited private right of action. One federal district court has interpreted it

---

[103] CAL. CIV. CODE § 1798.150(a). This section provides for liquidated damages of no less than $100 and no greater than $750 per incident, or actual damages if they are greater. *Id.* The CCPA also provides for injunctive or declaratory relief. *Id.*

[104] *Id.*

[105] CAL. CIV. CODE § 1798.81.5(d)(1)(A). The other types of personal information that may trigger a private right of action under the CCPA include a consumer's social security number, a government-issued identification number, credit or debit card information in combination with a security code allowing access to a bank account, medical information and health insurance information. *Id.*

[106] CAL. CIV. CODE § 1798.150(b).

[107] CAL. CIV. CODE § 1798.150(a)(1).

[108] CAL. CIV. CODE § 1798.81.5(b).

narrowly, dismissing a consumer's CCPA claim where the consumer failed to allege a security breach.[109] Another district court found that consumers stated a valid claim under the CCPA where the consumers alleged that their personal information "was viewed by unauthorized persons."[110] The court noted that the consumer-plaintiffs were not required to plead actual theft or unauthorized access.[111] It was enough that the plaintiffs' information was accessible to third parties via the Internet.[112] These cases provide preliminary guidance on how federal courts will apply the limited private right of action.

As a second level of enforcement, when a consumer cannot bring a private right of action, the CCPA vests enforcement power in the state attorney general.[113] The attorney general must notify the company that they are not in compliance with the CCPA and the allegedly noncompliant company will have 30 days to cure their violation.[114] If not, the noncompliant company will be liable for a civil penalty, the funds of which will be deposited in a Consumer Privacy fund used to offset the cost of enforcing the CCPA.[115]

3. State Laws Specifically Governing Biometric Privacy

Unlike the CCPA, which regulates many categories of personal information, three states have successfully enacted laws that protect individuals who share their biometric information with private companies: Washington, [116] Texas,[117] and Illinois.[118] Other states have proposed legislation, but unsuccessfully so.[119] Their lack of success is possibly a result of the unresolved issues with the current state of biometric privacy

---

[109] McCoy v. Alphabet, Inc., No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021).

[110] Stasi v. Inmediata Health Group Corp., No. 19cv2353 JM (LL), 2020 WL 6799437, at *16 (S.D. Cal. Nov. 19, 2020).

[111] *Id.*

[112] *Id.*

[113] CAL. CIV. CODE § 1798.155(b).

[114] *Id.*

[115] CAL. CIV. CODE § 1798.155(c).

[116] WASH. REV. CODE § 19.375.020.

[117] TEX. BUS. & COM. CODE ANN. § 503.001.

[118] 740 ILL. COMP. STAT. 14/10–/20.

[119] H.B. 2728, 54th Leg., 2nd Reg. Sess. (Ariz. 2020) (dead); H.B. 1153, 2019 Sess. (Fla. 2019) (died in committee); Mass. S.B. 120, 191st Sess. (Mass. 2019) (died in committee); H.B. 307, 2020 Reg. Sess. (Md. 2020); H.B. 4812, 123rd Sess. (S.C. 2020); H.B. 1417, 2020 Sess. (N.H. 2020) (dead); H.B. 4106, 2020 Reg. Sess. (W.V. 2020) (dead); H.B. 1153, 2019 Sess. (Fla. 2019) (died in committee); H.B. 645, 66th Leg., 2019 Reg. Sess. (Mont. 2019) (died in committee).

laws[120] or pushback from large companies looking to maintain cost-effective business practices.[121]

a. Illinois Biometric Information Privacy Act

Illinois is the first state to pass a biometric privacy law. To address the growth of biometric usage in business and the "heightened risk for identity theft," the Illinois legislature enacted the Illinois Biometric Information Privacy Act (BIPA).[122] The law was initially proposed in response to the downfall of Pay By Touch,[123] a California-based company that provided technology to supermarkets that allowed customers to complete transactions using their fingerprints.[124] Consumers, however, were unaware that it was Pay By Touch, the company behind the technology, rather than the supermarket, that was collecting their biometric data.[125] Despite security and convenience benefits, the biometric system of payment was "slow to catch on," and as a result, Pay By Touch machines were shut down and the company went bankrupt.[126] When Pay By Touch went bankrupt in 2008, it was unclear what would happen to consumers' biometric data.[127]

Concerned with consumer reluctance to "partak[e] in biometric-facilitated transactions" the Illinois legislature sought to alleviate concerns about the unknown "ramifications of biometric technology."[128] It did so by passing BIPA, which regulates the "collection, use, safeguarding, handling, storage,

---

[120] *See infra* Part II.

[121] *See e.g.*, Kartikay Mehrotra, *Tech Companies Are Pushing Back Against Biometric Privacy Laws*, BLOOMBERG (July 19, 2017, 8:26 PM), https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws [https://perma.cc/9BZE-GDS4]; *see also* Sara Morrison, *This Democrat and Ex-Microsoft Employee has a Federal Privacy Bill Republicans Might Actually Like*, VOX (Mar. 10, 2021, 5:00 AM), https://www.vox.com/recode/22301174/federal-privacy-bill-suzan-delbene [https://perma.cc/8VYF-ZGM7]; Luana Pascu, *New Hampshire Senate pushes back Biometric Information Protection Bill*, BIOMETRIC UPDATE (Jan. 9, 2020), https://www.biometricupdate.com/202001/new-hampshire-senate-pushes-back-biometric-information-protection-bill [https://perma.cc/8B6J-RVZK].

[122] 740 ILL. COMP. STAT. 14/5.

[123] Ill. H.R., 95th Gen. Assemb., 276th Leg. Day, Transcription Deb. at 249 (Ill. May 30, 2008) ("This Bill is especially important because one of the companies that has been piloted in Illinois, Pay By Touch, is the largest fingerprint scan system in Illinois and they have recently filed for bankruptcy . . . in March of 2008."); Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1098 (N.D. Ill. 2017).

[124] *See* Lowrey, *supra* note 12; Matt Marshall, *Pay By Touch in Trouble, Founder Filing for Bankruptcy*, VENTURE BEAT (Nov. 12, 2007, 2:09 PM), https://venturebeat.com/2007/11/12/pay-by-touch-in-trouble-founder-filing-for-bankruptcy/ [https://perma.cc/23B3-Z9V7].

[125] Jon Van & Becky Yurak, *Payment by Fingerprint Disappears*, CHI. TRIB. (Mar. 21, 2008), https://www.chicagotribune.com/news/ct-xpm-2008-03-21-0803200909-story.html [https://perma.cc/G2W8-U932].

[126] *Id.*

[127] Ill. H.R., 95th Gen. Assemb., 276th Leg. Day, Transcription Deb. at 249 (Ill. May 30, 2008); *Rivera*, 238 F. Supp. 3d at 1098.

[128] 740 ILL. COMP. STAT. 14/5.

retention, and destruction of biometric identifiers."[129] BIPA defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" and contains a list of personal information excluded from the definition.[130] BIPA also covers "biometric information" and defines it as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[131]

BIPA imposes five obligations on private entities that collect biometric identifiers or biometric information. Under Section 15(a), BIPA requires a private entity to develop a public written policy. The policy must establish a retention schedule and guidelines for permanently destroying biometric information once the purpose of collection has been satisfied or if the subject has not interacted with the entity for three years.[132] Section 15(b) requires the private entity to provide written notice to an individual whose biometric information is being collected and the purpose for collection and the individual must consent by execution of a written release.[133] Additionally, a private entity is prohibited from selling or profiting from, or disclosing, an individual's biometric identifier or information.[134] A private entity may disclose an individual's biometric identifier or information only if the individual consents or if disclosure is necessary to complete a transaction requested by the subject of the biometric identifier.[135] Finally, the statute imposes a duty on the entity to use the standard of care established within its respective industry to protect an individual's biometric identifier or information.[136]

Unlike other state biometric data privacy laws, BIPA grants an aggrieved individual a private right of action against a private entity that fails to abide by these requirements.[137] BIPA's private right of action provides: "[a]ny person aggrieved by a violation of [BIPA] shall have a right of action in a State

---

[129] *Id.*

[130] 740 ILL. COMP. STAT. 14/10. For example, "[b]iometric identifiers do not include 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." *Id.*

[131] *Id.*

[132] 740 ILL. COMP. STAT 14/15(a).

[133] *Id.*

[134] 740 ILL. COMP. STAT 14/15.

[135] 740 ILL. COMP. STAT 14/15(d).

[136] 740 ILL. COMP. STAT 14/15(e).

[137] 740 ILL. COMP. STAT. 14/20, An aggrieved individual is entitled to a minimum of $1,000 in damages for a negligent violation and a minimum of $5,000 for an intentional or reckless violation. *Id.*

circuit court."[138] In the landmark BIPA case, *Rosenbach v. Six Flags*, the Illinois Supreme Court interpreted the meaning of an "aggrieved" person for standing purposes. It held that any person whose biometric information is collected in violation of the statute, regardless of actual injury alleged, may bring an action against the allegedly noncompliant company.[139]

In *Rosenbach*, Stacey Rosenbach purchased a season pass to an amusement park on behalf of her son.[140] Upon her son's arrival at the park's security checkpoint, he scanned his thumbprint, which was then stored in the park's system.[141] Rosenbach brought an action under BIPA as an "aggrieved" person on the grounds that her son's biometric information was collected without consent and not in compliance with provisions laid out in Section 15(b) of BIPA.[142] In its defense, Six Flags argued that the petitioner was not "aggrieved" within the meaning of the law because her son had not suffered any injury as a result of the violation.[143] The Illinois Supreme Court held that under BIPA, "an individual need not allege some actual injury or adverse effect beyond violation of his or her rights under the Act in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief."[144] The court's broad interpretation of an "aggrieved individual" gives individuals the opportunity to police private entities' compliance with BIPA's mandates, which opens up these entities to expansive liability.

Following the *Rosenbach* decision, BIPA class action complaints have flooded Illinois state courts and federal district courts.[145] From September 2017 to December 2017, at least fifty entities "were affected by the filing of class action suits claiming" BIPA violations.[146] "In 2020, at least fifty four court rulings" mentioned BIPA, and in December 2020 alone thirty BIPA actions were filed.[147] In the mix of law suits, many well-known companies have been named in BIPA class actions,[148] including tech giants

---

[138] *Id.*

[139] Rosenbach v. Six Flags Entm't Corp., 129 NE.3d 1197, 1200, 1207 (Ill. S. Ct. 2019).

[140] *Id.*

[141] *Id.*

[142] *Id.* at 1201.

[143] *Id.* at 1201–02.

[144] *Id.* at 1207.

[145] Deal et al., *Rosenbach v. Six Flags Entm't Corp. – Illinois Supreme Court Takes Expansive View of Statutory Standing Under the Biometric Information Privacy* Act, 31 INTELL. PROP. & TECH. L.J. 17, 18 (2019) ("[O]ver 200 BIPA cases have been filed to date.").

[146] *See* MCCRAY, *supra* note 23, at 78.

[147] Tiffany Cheung et al., *Privacy Litigation 2020 Year in Review: BIPA Litigation*, MORRISON FOERSTER (Jan. 12, 2021), https://www.mofo.com/resources/insights/210111-bipa-litigation.html [https://perma.cc/ETB3-39SR].

[148] *See generally* Class Action Complaint, Robinson v. Petco Animal Supplies, Inc. (Ill Cir. Ct. Jan. 19, 2021) (No. 2021CH00273); Notice of Removal, Mcinnis v. Party City Corp. (N.D.

Facebook, Amazon, Microsoft.[149] These companies have paid millions in settlements to aggrieved consumers protected by BIPA.[150] Seeking to avoid a similar fate, companies doing business in Illinois are looking to defend against claims in a variety of ways, including challenging the categories of information that fall within BIPA, making dormant commerce clause challenges, and asserting lack of personal jurisdiction and Article III standing.[151] Law firms and data security companies are quickly populating the Internet with FAQs and "how-to-comply" guides to help companies not yet found to be in violation avoid a similar fate.[152]

b. Texas Capture or Use of Biometric Identifier Act

Within a year of Illinois, Texas became the second state to pass a biometric-specific privacy law. Texas's Capture or Use of Biometric Identifier Act (CUBI) has been dubbed "BIPA-lite" because of its relaxed consent and enforcement standards in

---

Ill. Jan. 19, 2021) (No. 1:21-cv-00309); Class Action Complaint, Payne v. Yum! Brands, Inc. (Ill Cir. Ct. Nov. 16, 2020) (No. 2020CH06811); Class Action Complaint, Hilliard v. Panera, LLC (Ill. Cir. Ct. Dec. 3, 2020) (No. 2020CH7056); Class Action Complaint, Acaley v. Vimeo, Inc. (Ill. Cir. Ct. Sept. 20, 2019) (No. 2019CH10873); Class Action Complaint, Flores v. Juul Labs, Inc. (Ill. Cir. Ct. Nov. 7, 2019) (No. 2019CH12935); Class Action Complaint, Nichols v. Whole Foods Mkt. Grp., Inc. (Ill. Cir. Ct. Aug. 6, 2019) (No. 2019CH09096); Class Action Complaint, Slate et al. v. Tik Tok, Inc. (N.D. Cal. Apr. 30, 2020) (No. 3:20-cv-02992-WHO); Class Action Complaint, Osborne v. WeWork Cos. (Ill. Cir. Ct. Nov. 5, 2019) (No. 2019CH12586); Class Action Complaint, Booker v. Hilton Mgmt., LLC. (Ill. Cir. Ct. Aug. 12, 2019) (No. 2019 CH09270).

[149] *See generally* Patel v. Facebook, 932 F.3d 1264 (9th Cir. 2019); Class Action Complaint, Ragsdale v. Amazon Web Srvs. (Ill. Cir. Ct. Nov. 5, 2019) (2019CH13251); Class Action Complaint, Vance v. Microsoft Corp. (No. 2:20-cv-01082) (W.D. Wash. July 14, 2020).

[150] In January 2020, Facebook offered to settle the class action suit initially for $550 million, but its offer was rejected by a judge. Nichola Iovino, *Judge Approves $650 Million Settlement in Facebook Biometric Case*, COURTHOUSE NEWS (Aug. 20, 2020), https://www.courthousenews.com/judge-approves-650-million-settlement-in-facebook-biometric-case/ [https://perma.cc/6F5L-NPQD]. Its $650 million settlement offer was approved in August 2020. *Id.* Walmart paid $10 million to Illinois employees alleging its palm reading device violated their privacy rights under BIPA. Lauren Zumbach, *Nearly 22,000 Illinois Walmart Workers Could Get a Share of $10 Million Privacy Settlement*, CHI. TRIB. (Jan. 19, 2021, 6:00 AM), https://www.chicagotribune.com/business/ct-biz-walmart-biometric-palm-scan-lawsuit-20210119-parcawurhzcshir2naurw5pccu-story.html [https://perma.cc/PZ68-DB2K].

[151] Charles Insler, *How to Ride the Litigation Rollercoaster Driven By The Biometric Information Privacy Act*, 43 S. ILL. U. L.J. 819, 822–24 (2019) (surveying different theories BIPA defendants are using to fight class actions).

[152] F. Paul Pittman & Abdul M. Hafiz, *Building a Robust Biometric Compliance Program in the US: A Five-Step Checklist*, WHITE & CASE (Nov. 9, 2020), https://www.whitecase.com/publications/alert/building-robust-biometric-compliance-program-us-five-step-checklist [https://perma.cc/N2PH-R8E3]; David J. Oberly, *Complying with The World's Most Stringent Biometric Privacy Law*, BLANK ROME (Jan.–Mar. 2020), https://www.blankrome.com/publications/complying-worlds-most-stringent-biometric-privacy-law [https://perma.cc/J2AR-J923]; Joseph Scharnak, *5 Tips for Keeping Your Association Complaint with the Illinois Biometric Privacy Act (Illinois)*, KOVITZ SHIFRIN NESBIT (Apr. 30, 2019), https://www.ksnlaw.com/blog/5-tips-bipa/ [https://perma.cc/KD9T-K2LS].

comparison to the Illinois law.[153] CUBI and BIPA differ in a few noticeable ways. Unlike BIPA, CUBI does not include a definition of "biometric *information*." It does, however, provide a definition of biometric *identifier*, which covers "a retina or iris scan, fingerprint, voiceprint or record of hand or face geometry."[154] CUBI requires private entities to inform individuals and obtain their consent before capturing their biometric information for a commercial purpose and imposes a reasonable care standard on the entity collecting the information.[155] Further, unlike BIPA's three-year destruction requirement, CUBI requires destruction within a reasonable amount of time, but no later than one year after the purpose for collection has expired.[156] Additionally, CUBI specifically regulates collection of biometric data for "commercial purpose[s]," but does not define that term,[157] suggesting that the statute has a broader reach. Further, unlike BIPA, CUBI does not require consent to be executed through a written release.[158] Finally, the primary distinction between BIPA and CUBI is enforcement: BIPA contains a private right of action whereas under CUBI, enforcement power lays only with the state attorney general.[159]

c. Washington Biometric Privacy Act

Washington is the third state to enact a biometric data privacy law. The Washington legislature found that Washington citizens were increasingly asked to provide their biometric information for "commerce, security and convenience purposes" and enacted the Washington Biometric Privacy Act (WBPA).[160] The WBPA defines a biometric identifier 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."[161] Unlike BIPA and CUBI,[162] Washington's statute does not include face or hand geometry scans in its definition of biometric

---

153 P. Russell Perdew et al., *Illinois's Biometric Information Privacy Act Spurs Similar Legislation Around the Country*, LOCKE LORD (Nov. 27, 2017), https://www.lockelord.com/newsandevents/publications/2017/11/~/media/162040E9E735479BB887E49BD0C91EF0.ashx [https://perma.cc/6FMD-BLW9]; John G. Browning, *The Battle Over Biometrics: A Look at The Law in Texas and Two Other States*, 81 TEX. BAR J. 674, 676 (2018).

154 TEX. BUS. & COM. CODE ANN. § 503.001(a) (emphasis added).

155 TEX. BUS. & COM. CODE ANN. § 503.001(b), (c)(2).

156 TEX. BUS. & COM. CODE ANN. § 503.001(c)(3).

157 TEX. BUS. & COM. CODE ANN. § 503.001(c)(1).

158 740 ILL. COMP. STAT 14/15(b) (2008).

159 740 ILL. COMP. STAT. 14/20; TEX. BUS. & COM. CODE ANN. § 503.001(d). The civil penalty for a violation under CUBI is $25,000. *Id.*

160 WASH. REV. CODE § 19.375.000.

161 WASH. REV. CODE § 19.375.010.

162 740 ILL. COMP. STAT. 14/10; TEX. BUS. & COM. CODE ANN. § 503.001(a).

identifier.[163] Instead, it defines biometric identifier as data derived by "measurements of an individual's biological characteristics" and includes fingerprints, voice prints, eye retinas, irises and "other unique biological patterns."[164] Further, the WBPA distinguishes between "enrolled" and "unenrolled" data.[165] The statute requires notice and consent to "enroll" data in a database, but these requirements do not apply to "unenrolled" data.[166]

The WBPA contains much of the same limitations on collection, retention, use and destruction of biometric information as both the Illinois (BIPA) and Texas (CUBI) laws. Similar to BIPA and CUBI, WBPA has notice and consent requirements for storing biometric data for commercial purposes; prohibits selling an individual's biometric data without consent; mandates a reasonable standard of care to protect against unauthorized access; and requires that the data only be stored for the amount of time necessary to serve the purpose for collection.[167] Like CUBI, the WBPA is enforceable by the attorney general and does not provide for a private right of action.[168] Because Washington's statute is limited to enrolled data[169] and does not have a private right of action, it is the least inclusive out of three existing state biometric privacy laws.

C. The "Biometric Bandwagon":[170] Proposed Biometric Privacy Laws

Many states have jumped on the biometric bandwagon, looking to follow in the footsteps of Illinois, Texas, and Washington by proposing some variation of a biometric privacy law.[171] At least twenty states have considered some form of biometric data legislation, over half of which provide a private right of action

---

[163] WASH. REV. CODE §19.375.010.

[164] *Id.*

[165] A biometric identifier is enrolled when an entity captures the data, converts it into a reference template, and stores it in a database that matches the biometric identifier to the individual. WASH. REV. CODE § 19.375.010(5).

[166] WASH. REV. CODE § 19.375.020(6).

[167] WASH. REV. CODE § 19.375.020.

[168] WASH. REV. CODE §19.375.030.

[169] Enrolled biometric data is biometric information that has been captured and converted "into a reference template that cannot be reconstructed into the original output image, and store[d] . . . in a database that matches the biometric identifier to a specific individual." WASH. REV. CODE §19.375.010(5).

[170] Molly K. McGinley & Kenn Brotman, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (March 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states [https://perma.cc/A3T9-NKA7].

[171] *See* MCCRAY, *supra* note 23; McGinley & Brotman, *supra* note 170; SHOLINKSY & HARRIS, *supra* note 44.

similar to that of BIPA.[172] For example, like BIPA, the proposed New York Biometric Privacy Act provides two private rights of action: one for negligent violations and another for intentional or reckless violations.[173] In contrast, the Arizona legislature modeled its proposed law on the WBPA, distinguishing between enrolled and unenrolled data.[174] The Missouri legislature has taken a more extreme approach by proposing criminal penalties for violating its biometric privacy law.[175] Further, at least two states have put forth biometric privacy laws whose application is limited to employers collecting employee biometric data.[176] Other states, like Connecticut and Arkansas, have decided to forego biometric-specific privacy legislation, and instead proposed amendments to include "biometric identifiers" within the definition of "personal information" laid out in their respective state's data breach law.[177]

In August 2020, Congress jumped on the biometric bandwagon and introduced a National Biometric Privacy Act (National Act).[178] The National Act, modeled after BIPA, provides an identical definition of biometric identifier.[179] It also provides the same rights to consumers. It requires a private entity in possession of biometric identifiers to develop, publicize, and comply with a written policy establishing a retention schedule; provides guidelines for destroying consumers' biometric identifiers; and mandates destruction of biometric identifiers, either when the initial purpose for collecting the biometric identifier has been

---

[172] H.B. 295, 2020 Sess. (Ala. 2020); H.B. 72, 13th Leg., 1st Gen. Sess. (Alaska 2017) (dead); H.B. 2728, 54th Leg., 2nd Reg. Sess. (Ariz. 2020); H.B. 350, 149th Gen. Sess. (Del. 2017); S.B. 1270, 2019 Reg. Sess. (Fla. 2019) (dead); H.B. 511, 62nd Leg., 2nd Reg. Sess. (Ida. 2014); S.B. 248, 120th Gen. Assemb., 2nd Reg. Sess. (Ind. 2018) (dead); S.B. 278, 2021 Reg. Sess. (Ky. 2021) (introduced); H.B. 218, 2021 Sess. (Md. 2021) (introduced); S.D. 269, 192nd Gen. Ct., 2021–22 Sess. (Mass. 2021); H.B. 5019, 99th Leg., 2017–2018 Sess. (Mich. 2017); H.B. 2375, 100th Gen. Assemb., 2nd Reg. Sess. (Mo. 2020); H.B. 645, 66th Leg. (Mont. 2019); H.B. 523, 2017 Reg. Sess. (N.H. 2017); A.B. 3625, 29th Leg., 2020 Reg. Sess. (N.J 2020); A.B. 27, 2021–22 Reg. Sess. (N.Y. 2021) (active); H.B. 5945, 2019 Gen. Assemb., Jan. Sess. (R.I. 2019); H.B. 4812, 2019–2020 Gen. Assemb., 123rd Sess. (S.C. 2020); H.B. 1215, 2020 Sess. (Va. 2020); H.B. 4106, 2020 Reg. Sess. (W.V. 2020).

[173] A.B. 27, 2021–22 Reg. Sess. (N.Y. 2021) (active).

[174] H.B. 2728, 54th Leg., 2nd Reg. Sess. (Ariz. 2020).

[175] H.B. 2375, 100th Gen. Assemb., 2nd Reg. Sess. (Mo. 2020).

[176] S.B. 824, 80th Leg. Assemb., 2019 Reg. Sess. (Or. 2019); H.B. 1215, 2020 Sess. (Va. 2020).

[177] H.B. 1943, 92nd Gen. Assemb., 2019 Reg. Sess. (Ark. 2019); H.B. 5310, 2021 Gen. Assemb., Jan. Sess. (Conn. 2021).

[178] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. (2020); *see also* Joseph L. Lazzarotti, *National Biometric Information Privacy Act, Proposed by Sens. Jeff Merkley and Bernie Sanders*, NAT'L L. REV. (Aug. 5, 2020), https://www.natlawreview.com/article/national-biometric-information-privacy-act-proposed-sens-jeff-merkley-and-bernie [https://perma.cc/CT8Q-KXBP].

[179] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 2(1).

satisfied, or within one year after the individual's last interaction with the entity, whichever comes first.[180]

Additionally, the National Act imposes limitations on collecting biometric data. An entity may only collect an individual's biometric data to provide a service for that person or for another "valid business purpose,"[181] which must be specified in a written policy regarding biometric data collection.[182] If the entity is collecting biometric information for another reason, the entity must inform the consumer that their biometric information is being collected and obtain a written release from the consumer.[183] Like BIPA, under the National Act, the entity must inform an individual that their biometric information is being collected and stored, and must inform them of the purpose thereof.[184] Further, consistent with the Illinois, Texas, and Washington laws, a private entity is prohibited from disclosing and selling or profiting from an individual's biometric information unless authorized to do so by the subject of the biometric identifier.[185] In complying with the law's mandates on collection, retention, use, and destruction, private entities are held to a reasonable standard of care.[186]

Like the CCPA, but unlike any other state biometric-specific law, the National Act explicitly provides the "right to know."[187] This right provides individuals the right to request from a business any information relating to the individual's data collected within the past year, free of charge.[188] Upon request, the entity must disclose to the individual

> [the following] categories of personal information; [] specific pieces of personal information; [] the categories of sources from which the business collected personal information; [] the purposes for which the business used the personal information; [and] . . . the categories of information that the business sells or discloses to third parties.[189]

Finally, the most widely debated provision is the private right of action. The National Act proposes that "[a]ny individual aggrieved by a violation of [this law] may bring a civil

---

[180] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(a).

[181] The National Act does not define "valid business purpose," but suggests that a valid business purpose is one published pursuant to the entity's written policy described in Section 3(a). National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(b).

[182] *Id.*

[183] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(b)(1).

[184] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(b)(1)(B).

[185] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(c); WASH. REV. CODE § 19.375.020; TEX. BUS. & COM. CODE ANN. § 503.001(c); 740 ILL. COMP. STAT 14/15(c).

[186] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(e)(1).

[187] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(f); CAL. CIV. CODE § 1798.110(a).

[188] National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 3(f).

[189] *Id.*

action . . . against a private entity" and "[a]ny such violation constitutes an injury-in-fact."[190] By expressly declaring a violation of the law an "injury in fact," the bill prospectively addresses the *Rosenbach* 'aggrieved individual' issue and anticipates Article III standing challenges, which have been inconsistently decided in BIPA cases brought in federal court.[191]

II. WHY A FEDERAL BIOMETRIC PRIVACY LAW IS NECESSARY

The wave of BIPA litigation following *Rosenbach* highlights two main issues with state biometric privacy laws.[192] First, although BIPA appears to provide a clear definition of biometric privacy to comprehensively protect consumer privacy rights, various lawsuits suggest that it may not be as straightforward as it appears.[193] Second, although BIPA provides a private right of action at the state level,[194] the ability to enforce this right on federal level may be curtailed by Article III standing.

A. Issues Defining "Biometric Information": Rivera v. Google

One fundamental issue with current biometric privacy laws is the varying statutory definitions of "biometric identifiers." Because biometric data collection is not a completely developed area of technology, states have discretion to define "biometric identifiers" differently, which may impact the level of protection individuals receive. For example, the BIPA definition of "biometric identifier" includes face and hand geometry scans, whereas the WBPA definition of "biometric identifier" does not.[195] Additionally, some states have proposed laws that choose to limit biometric data protection to only facial recognition, choosing to forego protection of other biometric identifiers like fingerprints, retina scans and voiceprints.[196] The issue with differing statutory definitions among states is that it grants unequal consumer protections solely based on jurisdiction. For instance, an Illinois resident whose face and hand geometry has

---

190 National Biometric Privacy Act of 2020, S. 4400, 116th Cong. § 4(a).

191 *See supra* Section. I.B.3.a.

192 *See* Insler, *supra* note 151, at 822–24.

193 *See generally* Rivera v. Google, 238 F. Supp. 3d 1088 (N.D. Ill. 2017); Monroy v. Shutterfly, Inc., 2017 WL 4099846, at *2 (N.D. Ill. Sept. 15, 2017); *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2016).

194 740 ILL. COMP. STAT. 14/20.

195 740 ILL. COMP. STAT. 14/10; WASH. REV. CODE §19.375.010.

196 H.B. 5326, 2016 Gen. Assemb., Feb. Sess. (Conn. 2016) ("'[B]iometric identifier' means a record of facial geometry, including, but not limited to, an image of an individual's face captured and stored utilizing facial recognition software.").

been collected and retained without consent has redress under BIPA, but a Washington resident may have no redress at all. This is not a sound basis for differentiating levels of privacy protection, as all consumers should receive the same level of protection when they place the fate of their biometric information in the hands of a business.

Additionally, underinclusive definitions allow courts to fashion their own definitions, at the risk of crossing the legislative-judicial line. *Rivera v. Google* illustrates this problem. *Rivera* involved a class of plaintiffs who brought suit against Google for using their facial geometry without their knowledge and consent, in violation of BIPA.[197] The individuals photographed themselves using a Google Android device and the photographs were then automatically uploaded to a cloud-based photo service where Google software recognized the individuals and grouped them together in photos.[198] The plaintiffs brought suit in the Northern District of Illinois against Google, alleging that Google used their facial geometry derived from their photographs, which falls within the meaning of "biometric identifier" under BIPA.[199] The issue in *Rivera* was whether the information collection was considered a photograph, to which BIPA does not apply, or a facial geometry scan, to which BIPA does apply.[200] The court held that the facial templates collected by Google qualified as biometric identifiers and therefore the plaintiffs successfully stated a claim under BIPA.[201] Based on the interpretation of the statute, the method used to collect biometric identifiers is immaterial.[202] The court explained that "a 'biometric identifier' is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component used to identify a person."[203]

Additionally, varying definitions of biometric identifiers compel all businesses, large and small, to comply with the most expansive definition, even in states without biometric privacy statutes. In Google's briefings in *Rivera*, it argued that a ruling against Google would force it to comply with BIPA, regardless of where the individual using the Google software resides, in order to

---

197 *Rivera*, 238 F. Supp. 3d at 1091.

198 *Id.*

199 *Id.*; 740 ILL. COMP. STAT. 14/10.

200 *Rivera*, 238 F. Supp. 3d at 1092–93.

201 *Id.* at 1094–95.

202 *Id.*

203 *Id.* at 1096; *see also* Monroy v. Shutterfly, Inc., 2017 WL 4099846, at *3 (N.D. Ill. Sept. 15, 2017).

avoid potential liability nationwide.[204] The "practical effect" would be that BIPA regulates conduct taking place outside of Illinois.[205] Google framed this as a dormant commerce clause issue,[206] however, looking beyond the constitutional implications, the effect of a single state law would induce businesses to develop costly compliance systems to ensure protections for *all* consumers. Realistically, businesses are not going to parse through each individual consumer's biometric identification to determine whether they are from Illinois, Washington, Texas, or a nonregulated state. As such, as Google argued, either businesses will face prohibitively expensive compliance costs or be governed by the broadest state definition, even though other states have chosen a narrower definition, or none at all.

B. The Great BIPA Debate: Article III Standing

The second, and most complex issue, arising from BIPA is whether consumers have Article III standing to bring a BIPA suit in federal court.[207] Article III standing is one of the most widely discussed issues in biometric privacy law litigation. The prevailing view is that a federal biometric privacy law should be modeled after BIPA, specifically because it provides a private right of action.[208] There has been much debate, however, as to

---

[204] Google Inc.'s Memorandum of Law in Support of Its Consolidated Motion to Dismiss Plaintiff's First Amended Complaints Pursuant to Fed. R. Civ. P. 12(b)(6) at 16, Rivera v. Google, Inc. 238 F. Supp. 3d 1088 (2017) (No. 1:16-cv-02714).

[205] *Id.*

[206] *Id.* at 16–17.

[207] Article III of the Constitution provides that federal courts jurisdiction is limited to actual "Cases . . . or . . . Controversies." U.S. Const. art. III., § 2. The Supreme Court has interpreted this to mean that it is not constitutionally permitted to issue a binding decision unless three requirements have been met: first, the plaintiff has suffered an injury in fact—"an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical;" second, the injury must be "fairly traceable" to the alleged action of the defendant; and third, it must be "likely," rather than "speculative," that the injury will be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992) (internal citations omitted). Therefore, a federal court hearing a BIPA claim brought by an individual against a private entity would need to find that the alleged violation caused an injury that is actual or imminent.

[208] *See* Blake Benson, *Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy*, 19 N.C. J. L. & TECH. 161, 180 (2019) ("Adding a private right of action will give the [federal] law the 'teeth' that detractors of Texas and Washington's laws are clamoring for . . . ."); Chloe Stepney, *Actual Harm Means it Is Too Late: How* Rosenbach v. Six Flags *Demonstrates Effective Biometric Privacy Law*, 40 LOY. L.A. ENT. L. REV. 51, 86 (2019) (proposing that a federal regulation should provide consumers with a private right of action to hold companies accountable); Zimmerman, *supra* note 52, at 670 ("[T]he [biometric privacy statute] should provide a private cause of action for consumers . . . ."); Ian Taylor Logan, *For Sale: Window to the Soul Eye Tracking as The Impetus For Federal Biometric Data Protection*, 123 PENN ST. L. REV. 779, 810 (2019) ("[A] private right of action is of tantamount importance if the statute is to have any commendable impact."). *But see* Stewart, *supra* note

whether a private right of action conforms with Article III standing requirements when a BIPA claim is brought in federal court. While some have put forth that BIPA claims in federal court bypass Article III standing, others assert that a mere violation of any BIPA provision, without any actual harm alleged, is a violation of a substantive privacy right in itself. This issue foreshadows a potential problem with a private right of action in a federal biometric privacy law.

Spokeo v. Robbins sets the standard for alleging a concrete injury in a case governed by a statutory cause of action, such as BIPA. In *Spokeo*, the Supreme Court clarified the distinction between statutory violations that cause harm and "bare procedural violations" that do not entail "a degree of risk sufficient to meet the concreteness requirement."[209] Injury-in-fact, however, is not satisfied just because a statute grants an individual a statutory right and provides that individual with a private right of action.[210] The violation must be accompanied by a real injury or a risk of real harm, even if that harm is intangible.[211] Applying this framework, a consumer bringing a private right of action in federal court under BIPA must plead some tangible or intangible injury or risk of harm resulting from a statutory violation of the statute.

Is a BIPA violation merely a procedural violation that renders a private right of action brought in federal court impossible? The Ninth Circuit addressed this issue in *Patel v. Facebook*. There, the Ninth Circuit held that Facebook users whose facial geometry was collected without knowledge and consent alleged a concrete injury-in-fact for purposes of Article III standing.[212] In *Patel*, Facebook users in Illinois challenged Facebook's "Tag Suggestions" feature, which is technology that "extracts the various geometric data points that make a face unique[,] . . . then compares the face signature to faces in

---

52, at 385 (proposing a federal law be modeled after the WBPA (Washington state's biometric privacy statute), which does not provide for a private right of action).

[209] Spokeo, Inc. v. Robbins, 136 S. Ct. 1540, 1549–50 (2016). In *Spokeo*, Plaintiff, a consumer, brought suit under the Fair Credit Reporting Act (FCRA) upon learning that the Defendant, a credit reporting agency, posted inaccurate information about the Plaintiff on its people search engine. *Id.* at 1540, 1544. The FCRA requires consumer reporting agencies to follow certain procedures to "ensure 'fair and accurate credit reporting.'" *Id.* at 1545; 15 U.S.C. § 1681(a)(1). The court held that the Plaintiff needed to allege more than just a procedural violation of the statute to meet the injury-in-fact requirement and remanded the case to determine if the Plaintiff had properly done so. *See Spokeo*, 136 S. Ct. at 1549–50.

[210] *Spokeo*, 136 S. Ct. at 1547–49 ("[I]t is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.").

[211] *Id.* at 1549.

[212] Patel v. Facebook, 932 F.3d 1264, 1267 (9th Cir. 2019).

Facebook's database of user face templates" and "[i]f there is a match between the face signature and the face template, Facebook [] suggest[s] tagging the person in the photo."[213] On the standing issue, the court adopted a two-step approach to determine whether a statutory violation causes concrete injury.[214] First, the court asks "whether the statutory provisions at issue were established to protect [the plaintiff's] concrete interests (as opposed to purely procedural rights) and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests."[215] Turning to the first prong, the Ninth Circuit relied on the Illinois Supreme Court's interpretation of BIPA in *Rosenbach*—namely that an individual is "aggrieved" when a private entity fails to comply with its obligation under BIPA—and concluded that BIPA was enacted to "protect an individual's 'concrete interests' in privacy, not merely procedural rights."[216] For the second prong, the Ninth Circuit again deferred to the *Rosenbach* Court, finding a material risk of harm when an individual's biometric information is collected without knowledge and consent.[217] It reasoned, briefly, that BIPA's procedural protections "are particularly crucial in our digital world" and "[w]hen a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air."[218]

The Seventh Circuit, however, has found that not all BIPA violations create an injury that is individualized and concrete enough to meet the Article III injury-in-fact requirement.[219] In *Bryant v. Compass Group USA, Inc.*, the Seventh Circuit held that the plaintiff had standing to bring a BIPA claim where plaintiff alleged a company's failure to meet BIPA's notice and consent requirements, but did not have standing with respect to the company's alleged failure to provide a publicly available retention schedule.[220] In that case, plaintiff

---

[213] *Id.*

[214] *Id.*

[215] *Id.* at 1270–71.

[216] *Id.* at 1274.

[217] *Id.*

[218] *Id.*

[219] *See generally* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020); Fox v. Dakkota Integrated Sys., 980 F.3d 1146 (7th Cir. 2020); Thornley v. Clearview AI, 984 F.3d 1241 (7th Cir. 2021).

[220] *Bryant*, 958 F.3d at 624, 626. In *Bryant*, Plaintiff used her fingerprint to create an account that would allow her to purchase food from a vending machine at her place of employment. *Id* at 619. Defendant, the vending machine provider, never publicly made a retention schedule or any guidelines for destroying biometric identifiers or

used her fingerprint to create an account that would allow her to purchase snacks from a vending machine at her place of employment.[221] Compass Group (Compass) removed the case to federal court.[222] Notably, the plaintiff moved to remand the action back to state court, casting doubt on her own ability to establish the concrete injury-in-fact element necessary for Article III standing, which is not necessary in order to bring an action in Illinois state courts.[223] To resolve the standing question, the Seventh Circuit cited *Spokeo* and held that to show a concrete injury-in-fact there must be some "appreciable risk of harm" to the interests protecting by the statute.[224]

Unlike the Ninth Circuit in *Patel*, the Seventh Circuit accorded less deference to the Illinois Supreme Court in *Rosenbach*. It reasoned that state standing requirements are "more lenient than those imposed by Article III."[225] Nonetheless, the court likened Bryant's injury to a concrete injury in the sense that failure to comply with BIPA, although not a "tangible injury," is an "invasion of [one's] private domain" similar to "an act of trespass."[226] By failing to inform Bryant and obtain her consent to collect, use, and store her biometric information, Compass deprived her of "the opportunity to make informed choices about to whom and for what purpose they will relinquish control of that information."[227] The court considered, however, the retention policy violation separately. Because the obligation to develop a written retention policy is one owed to the public rather than to a particular person whose biometric identifier or information was collected, there was no particularized harm.[228] Therefore, she lacked Article III standing to allege a violation under that section.

A few months later, the Seventh Circuit seemingly contradicted its holding in *Bryant*. In *Fox v. Dakkota Integrated Systems*, the court held that an entity's failure to publicly disclose and develop a data retention schedule with guidelines for permanent destruction was an injury-in-fact sufficient to support the plaintiff-employee's Article III standing.[229] It

---

information it was collecting or storing, nor had the company ever informed Plaintiff her fingerprint was being collected or stored. *Id.*

[221] *Id.* at 619.

[222] *Id.* at 620. The case was removed to federal court on the basis of diversity of citizenship and an amount-in-controversy of $5 million. *Id.*

[223] *Id.*

[224] *Id.* at 621.

[225] *Id.*

[226] *Id.* at 624.

[227] *Id.* at 626.

[228] *Id.*

[229] Fox v. Dakkota Integrated Sys., 980 F.3d 1146, 1154 (7th Cir. 2020).

reasoned that, unlike the plaintiff in *Bryant*, the plaintiff in *Fox* alleged that the private entity

> violat[ed] the full range of its section 15(a) duties by failing to develop, publicly disclose, *and comply with* a data-retention schedule and guidelines for the permanent destruction of biometric data when the initial purpose for collection ends . . . result[ing] in the unlawful retention of her handprint . . . and the unlawful sharing of her biometric data with [a] third-party database administrator.[230]

The court's ruling suggests that the failure to implement data retention and destruction protocols set out in the retention schedule is harm just as concrete as the failure to provide notice and consent.[231] The Seventh Circuit seemed to distinguish *Bryant* not based on the particular provision of BIPA that was violated, but on the way in which the plaintiff artfully pled an alleged violation of that provision. Given the importance of protecting and asserting biometric privacy rights, these cases give consumers—and courts—little guidance on when a plaintiff has met Article III standing requirements. Such unpredictability may be attributed to the vague, and consequently limitless, language provided for in BIPA's private right of action.

III. SOLUTION: A CALL FOR A FEDERAL BIOMETRIC DATA PRIVACY LAW

Biometric technology development and use is advancing rapidly and it is difficult, if not impossible, to predict how stolen biometric data may be used.[232] Although some state legislatures have attempted to protect individuals from these speculative risks,[233] a patchwork of state laws regulating biometric data is not sufficient to protect individuals' highly sensitive information. Compliance with state laws would require companies to evaluate their data protection policies under each individual state statute[234] or otherwise follow a *de facto* federal law governed by BIPA, which would flood federal courts with litigation. Therefore, to address the issues that arise from BIPA, and in anticipation of increased use of biometric data, Congress should enact a federal statute modeled after the CCPA to protect consumers. Although the CCPA reaches far beyond just biometric data, it can be used as a model for a law

---

230 *Id.*

231 *Id.* at 1155.

232 *See* Tsai, *supra* note 15; 740 ILL COMP. STAT. 14/5(f).

233 740 ILL COMP. STAT. 14/5(f).

234 Eric Goldman, *What We've Learned from California's Consumer Privacy Act so far*, HILL (Jan. 11, 2020, 2:00 PM), https://thehill.com/opinion/cybersecurity/477821-what-weve-learned-from-the-california-consumer-privacy-act-so-far [https://perma.cc/9HEA-4E4B].

specifically governing biometric data on a federal level because of its broad definition of biometric identifier, its limitations on a private right of action, and the balance it strikes between protecting consumer information and addressing business' cost concerns.

As demonstrated through the above discussion highlighting the challenges arising out of BIPA, the primary rationales behind a federal law are the need for a single, yet broad definition for the type of biometric identifiers protected under the law and a resolution of the standing issue presented by a limitless private right of action. A federal law, called The Federal Biometric Privacy Act, would contain a broad definition of "biometric identifier;" the right to know; the right to opt-out; the right to delete; and a limited private right of action shared with enforcement power in the attorney general.

A. Defining Biometric Information Broadly

First, the Federal Biometric Privacy Act would adopt the clearest and most expansive definition of "biometric information." The CCPA definition contains a clear list of biological and behavioral characteristics in its definition, eliminating the possibility of debating what constitutes biometric identification.[235] The CCPA definition also has the farthest reach in the different types of biometric identifiers it covers.[236] "Biometric information" under the CCPA includes "physiological, biological, and behavioral characteristics" and "imagery" of an individual's iris, palm, or vein patterns if an "identifier template" can be derived therefrom, whereas BIPA does not explicitly include this language.[237] This definition responds to the dispute in *Rivera* over whether "photographs" are biometric identifiers. As the *Rivera* court protected biometric data regardless of the underlying method by which it was collected, a uniform federal law should protect irreplaceable personal biological information.

Furthermore, the CCPA definition also considers keystroke patterns and rhythms, which have recently been studied as a potential method of biometric identification.[238] BIPA does not address the possibility that a consumer can be identified this way.[239] Finally, like the CCPA the definition should include an expansive, but non-exhaustive list of biometric

---

[235] *See* CAL. CIV. CODE § 1798.140(b).

[236] *See* CAL. CIV. CODE §§ 1798.125, .140.

[237] *See* McGinley & Brotman, *supra*, note 170 ; CAL. CIV. CODE §§ 1798.140, .150; 740 ILL COMP. STAT. 14/10.

[238] CAL. CIV. CODE §§ 1798.125, .140.

[239] *See* Seha & Abo-Zahhad, *supra* note 9.

identifiers to embrace the possibility of future technological developments.[240] A broader definition provides for longevity of the statute and accounts for the unknown risks associated with stolen biometric data that have not been fully realized.[241]

B. Consumer Rights Under A Federal Law

The Federal Biometric Privacy Act should grant individuals a "right to know" what biometric information is being collected about them, a "right to opt-out" of having their data collected, and a right to request that an entity erase your biometric data from its system, also known as the "right to delete."

The "right to know" should mirror the CCPA's requirement that companies disclose to consumers the categories of personal information that the business collected.[242] The proposed federal law would require that private entities disclose the biometric information they collect from consumers.[243] This right contrasts with the Illinois, Texas, and Washington statutes that require companies to obtain explicit consent from consumers before collecting their biometric data.[244] The federal law should contain a provision mandating private entities inform consumers of biometric information collection. Once the consumer has been informed, consent is implied. This requirement weighs both the need to protect an individual's privacy rights and the need for cost-efficient and secure business practices.

A "right to opt out"—rather than opt-in—requiring explicit consent, like BIPA and other proposed state biometric privacy laws, presumes a consumer's informed consent. It requires individuals with knowledge that a private entity has collected their information to inform the entity that they do not want their biometric information to be stored. Commentators argue that the right to opt-in is "truly fundamental" to a federal biometric privacy law.[245] Although an opt-out favors data collection over privacy rights,[246] to require private entities to obtain affirmative consent would lead to prohibitively expensive compliance costs.[247]

---

[240] 740 ILL COMP. STAT. 14/5(f) ("The full ramifications of biometric technology are not fully known."); Rivera v. Google, Inc. 238 F. Supp. 3d 1088, 1096 (2017) ("Who knows how iris scans, retina scans, fingerprints, voiceprints, and scans of faces and hands will be taken in the future?").

[241] *See* Logan, *supra* note 208, at 809.

[242] *See* CAL. CIV. CODE § 1798.100 (2018).

[243] *Id.*

[244] 740 ILL. COMP. STAT. 14/15 (2008); WASH. REV. CODE § 19.375.020 (2017); TEX. BUS. & COM. CODE ANN. § 503.001(b) (2017).

[245] *See* Logan, *supra* note 208, at 808.

[246] *Id.*

[247] Alan McQuinn and Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFO. TECH. & INNOVATION FOUND. (Aug. 5, 2019), https://itif.org/publi

Given technology's prevalence in our society, most people have at some point provided their fingerprint or other biometric identifier to a company, and feel somewhat comfortable doing so.[248] The discomfort arises when consumers feel that their individual privacy has been invaded and they have lost control over the information they provided.[249] As such, consumers should have the right to exclude companies from retaining this information, even if they had previously allowed their biometric information to be collected. Put simply, the right to disallow companies to retain biometric information should accompany the right to allow its collection in the first place. Therefore, a federal law with a right to opt-out strikes a balance between protecting individual privacy and encouraging cost-effective business practices, as ensuring that all consumers have properly consented can cost companies millions to ensure compliance.[250]

The "right to delete" should give individuals the right to request that the private entity, to whom they gave their information, remove that information from their database. Similar to the right to delete in the CCPA, the federal statute should provide this right by allowing individuals to request that the private entity dispose of their biometric data.[251] Such a right is fundamental to any consumer privacy law because it allows individuals autonomy over the information derived from their unique biological and behavioral characteristics.[252] Additionally, like the CCPA, the right to delete in a federal biometric privacy law would be subject to exceptions that free businesses from their obligation to delete consumer information upon request.[253] While these exemptions weigh against an individual's autonomy over their biometric information, they weigh in favor of business security and functionality. For example, as

---

cations/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law [https://perma.cc/XUH7-AJKZ].

[248] *See* GERMAN & BARBER, *supra* note 11, at 7 (finding that "from 68%–76% of respondents said they were either very comfortable or somewhat comfortable with each of the biometric types").

[249] *Id.* at 15.

[250] The E.U.'s privacy law, the GDPR, requires explicit consent to collection of personal information and has been criticized as compliance has become extremely expensive. *See* Oliver Smith, *The GDPR Racket Who's Making Money From This $9bn Business Shakedown*, FORBES (May 2, 2018, 2:30 AM), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/?sh=6d972b3034a2 [https://perma.cc/A56K-KPS8] (reporting that Fortune 500 companies in the United States have spent a combined $7.8 billion to comply with a strict European privacy law requiring explicit consent).

[251] CAL. CIV. CODE § 1798.105.

[252] *See Majorities Say Americans Should Have Right to Have Certain Information Held by Other People or Organizations Permanently Deleted*, PEW RES. CTR (Jan. 27, 2020), https://www.pewresearch.org/fact-tank/2020/01/27/most-americans-support-right-to-have-some-personal-info-removed-from-online-searches/ft_2020-01-27_rtbf_03/ [https://perma.cc/Q63F-85BN].

[253] CAL. CIV. CODE § 1798.105.

identified above, one CCPA exception does not require a business to comply with the right to delete if retaining that person's information is necessary to detect security incidents.[254] Such an exception allows businesses to override an individual's privacy rights to protect themselves from incidents such as data breaches, which are a primary concern of consumers. Another example is the exemption for "repair[ing] errors that impair existing intended functionality."[255] This exception acknowledges that a business may rely on the retention of personal data in its normal function.[256] Modeling a federal right to delete after the CCPA considers that such a right should not overburden a business in a way that impairs its functionality when it relies on retaining biometric data.

C. A Limited Private Right of Action

Finally, consistent with the prevailing view, the Federal Biometric Privacy Act should include a private right of action; however, like the CCPA, it should be limited. A limited private right of action provides plaintiffs with more predictability in the outcome of cases raising Article III standing issues. The clear language encourages plaintiffs to allege some injury beyond a mere statutory violation by requiring aggrieved plaintiffs to allege that the failure *subjected* their biometric information to unauthorized access or disclosure. Additionally, like the CCPA, the private right of action under the federal law would grant businesses a comfortable thirty-day cure period. The thirty-day cure period opportunity has led to increased compliance among businesses collecting personal information in California.[257] This is an amendment to BIPA that the Illinois legislature is considering, possibly as an effort to curb the flood of litigation in Illinois state and federal courts.[258]

Additionally, like the CCPA, the Federal Biometric Privacy Law should contain a provision that gives enforcement power to the Attorney General.[259] If a company is found to simply have violated the federal procedures required by the law, but an individual bringing suit against the company has not alleged any

---

[254] CAL. CIV. CODE § 1798.105(d)(2).

[255] CAL. CIV. CODE § 1798.105(d)(3).

[256] Notably, this exception applies to a business's *existing* functionality. *Id.* This implies that a business is still obligated to delete the consumer's information upon request if data is being used for a new functionality.

[257] Press Release, State of Cal. Dep't of Justice, Attorney General Becerra Announces Approval of Additional Regulation That Empowers Data Privacy Under the California Consumer Privacy Act (Mar. 15, 2021), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data [https://perma.cc/XNE4-CRV5].

[258] *See* H.B. 559, 102 Gen. Assemb., 2021–2022 Sess. (Ill. 2021).

[259] CAL. CIV. CODE § 1798.155.

harm or risk of harm for said violation, not only would the individual lack Article III standing, but the company may be exposed to billions of dollars in damages.[260] Such a provision would not fairly balance the benefits of biometric data usage with an individual's right to privacy. Understanding that these companies should still be held accountable, the federal biometric privacy law leverages the attorney general enforcement power by affording any business or third party the option to seek compliance guidance from the attorney general. If the attorney general finds that a business is not compliant and it fails to cure the violation, the business will be subject to a civil penalty for each violation.[261] This provision provides another layer of protection where a plaintiff cannot show imminent harm, but a company is held accountable for violating a procedural provision of the statute.

Alternative to attorney general enforcement, Congress should consider the creation of an administrative agency to address privacy violations. If a private entity violates the Federal Biometric Privacy Act, or any federal privacy law, the aggrieved individual may file a complaint with the agency. The independent agency would then launch an investigation, and, if warranted, bring an action against the private entity on behalf of the aggrieved individual. It has been suggested that the Federal Trade Commission (FTC)[262] is the proper entity to enforce a federal biometric privacy law, however, this is not feasible.[263] The FTC also has the authority to find that a business that suffered a data breach as a result of inadequate privacy protections has engaged in unfair business practices.[264] It can bring an action against businesses that suffered data breaches on the ground that the business engaged in "unfair practices" by failing to adequately secure consumer information.[265] Despite this broad authority, it is likely that the FTC would only investigate "the most egregious and expansive data breaches."[266]

---

[260] Brief of Amicus Curiae Illinois Chamber of Commerce in Support of Defendants-Appellees Six Flags Entm't Corp. and Great America LLC at 10, Rosenbach v. Six Flags Entm't Corp., 129 NE.3d 1197 (Ill. S. Ct. 2019) (No. 123186).

[261] CAL. CIV. CODE § 1798.155.

[262] The FTC has the authority to regulate the consumer industry through investigating unfair business practices, seeking relief on behalf of injured consumers, and establishing guidelines for fair business practices. *What We Do*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/what-we-do [https://perma.cc/3KRA-YLBM].

[263] *See* Zimmerman, *supra* note 52, at 637–40.

[264] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 249 (3d Cir. 2015) ("Our conclusion is this: that the FTC later brought unfairness actions against companies whose inadequate cybersecurity resulted in consumer harm is not inconsistent with the agency's earlier position.").

[265] *Id.* at 240.

[266] *Id.*

Enforcement only in the event of major violations is not sufficient given the unique and irreplaceable nature of biometric identifiers.

The entity most equipped to handle privacy violations may be one that does not yet exist. The Federal Biometric Privacy Act should authorize the creation of a new independent agency to regulate all privacy violations in the private sector. This agency would mirror the information commissions established in many other countries. For example, Canada has the Officer of the Privacy Commissioner of Canada[267]; France has the National Commission on Informatics and Liberty (CNIL);[268] and the UK has the Information Commissioner's Office.[269] Under the Federal Biometric Privacy Act, an individual who believes their biometric information was not collected in compliance with the statute could file a complaint with the commission.

CONCLUSION

The legal landscape of data privacy law is missing both a general federal privacy law and a biometric privacy law. Though the CCPA is the first state-level comprehensive privacy law, its protections which extend beyond biometric data, Congress should focus on a privacy law that specifically governs biometric privacy. Given the irreplaceable and unique nature of biometric data, individuals are putting their unique and irreplaceable information at unknowable risk. Acknowledging that general personal information deserves protection, the consequences of stolen data are not as dire as they are for biometric information.

Further, although protecting biometric privacy is imperative, it must be weighed against the benefits of biometric data usage. Collecting data allows companies to improve consumer experience, increase security, and cut overhead costs. A federal law with a limitless private right of action, such as that in BIPA, would undercut these objectives. To many, a limitless private right of action seems to be the most logical and direct remedy. It would, however, be economically infeasible, flood federal courts with litigation, and raise serious questions about Article III standing jurisprudence. As more comprehensive biometric privacy laws are introduced, businesses will be forced

---

[267] *About the OPC*, OFF. PRIVACY COMMISSIONER OF CANADA, https://www.priv.gc.ca/en/about-the-opc/ [https://perma.cc/4GR6-K9VF].

[268] *The CNIL'S Mission*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, https://www.cnil.fr/en/cnils-missions [https://perma.cc/YZW9-SNK3].

[269] *Your Data Matters*, INFO. COMMISSIONER'S OFF., https://ico.org.uk/your-data-matters/.

to invest in personnel to ensure compliance, or states would race to pass the strictest biometric privacy law that sets a national standard. The state with the strictest biometric privacy law should not govern the limitations on privacy rights of all individuals. Regulating and protecting consumers' biometric privacy is a job best left for the legislature.

Eliza Simons[†]

[†] J.D., Brooklyn Law School, 2021; B.A. Tulane University, 2018. Thank you to the entire *Brooklyn Law Review* executive board and staff for their hard work and dedication to this publication, despite a challenging time amid the pandemic. Thank you to my family and friends for their endless patience, encouragement support through the writing process. Finally, a special thank you to my grandfather Arthur Simons '58 for inspiring me to pursue a career in law. I would not be where I am today without you.