Duquesne Law Review

Volume 59 | Number 2 Article 7

2021

# The Future of Our Fingerprints: The Importance of Instituting Biometric Data Protections in Pennsylvania

Julia M. Siracuse

Follow this and additional works at: https://dsc.duq.edu/dlr

 Part of the Privacy Law Commons

Recommended Citation
Julia M. Siracuse, *The Future of Our Fingerprints: The Importance of Instituting Biometric Data Protections in Pennsylvania*, 59 Duq. L. Rev. 303 (2021).
Available at: https://dsc.duq.edu/dlr/vol59/iss2/7

This Student Article is brought to you for free and open access by the School of Law at Duquesne Scholarship Collection. It has been accepted for inclusion in Duquesne Law Review by an authorized editor of Duquesne Scholarship Collection.

# The Future of Our Fingerprints: The Importance of Instituting Biometric Data Protections in Pennsylvania

*Julia M. Siracuse**



* J.D. Candidate, Duquesne University School of Law, 2021. The author received her Bachelor of Arts with a double major in Chinese and Sociology from the University of Pittsburgh in 2018. She thanks her parents and brothers for their constant support and Professor Ann L. Schiavone for her invaluable guidance and encouragement.

## I. INTRODUCTION

Only a few years ago, people would not have thought about using fingerprints or facial recognition to operate a cell phone.[1] Today, these are common features of smartphones that make our lives more efficient and straightforward.[2] These fingerprints and facial recognition features used on smartphones are two examples of a specific type of sensitive data known as biometric data: data that uniquely identifies an individual according to their own physical and behavioral attributes.[3] The scope of biometric data technology is rapidly expanding, resulting in an accumulation of more aspects of daily life revolving around data.[4] Institutions and services that people interact with daily—including social media, banking, retail, and government—now involve the collection and analysis of biometric data.[5] While the implementation of biometric data across these industries has benefits, it comes with substantial risks as well, which must be effectively managed.[6] Individuals, companies, and other entities must understand that biometric data can be hacked by cyber criminals.[7] Today, if an individual's credit card or social security number is stolen, they have the ability to set up a new one.[8] One cannot, however, replace a stolen fingerprint or DNA sample.[9]

---

1. *See* Vindu Goel, *That Fingerprint Sensor on Your Phone Is Not as Safe as You Think*, N.Y. TIMES (Apr. 10, 2017), https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html (stating that fingerprint scanners have turned today's smartphones into miracles of convenience).

2. Riley v. California, 573 U.S. 373, 395 (2014) ("Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower . . . . Today . . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

3. *See* Maria Korolov, *What Is Biometrics? 10 Physical and Behavioral Identifiers That Can Be Used for Authentication*, CSO (Feb. 12, 2019, 3:00 AM), https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html.

4. Leonardo Sam Waterson, *10 Ways Biometric Technology Is Implemented in Today's Business World*, M2SYS (Nov. 29, 2018), http://www.m2sys.com/blog/biometric-technology/10-ways-biometric-technology-implemented-business/.

5. Danny Palmer, *What Is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZDNET (May 17, 2019, 6:33 AM), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

6. *See* Scott Sayce, *Cyber Security: The Future Risk of Biometric Data Theft*, CNA HARDY, https://www.cnahardy.com/news-and-insight/insights/english/cyber-securit-the-future-risk-of-biometric-data-theft (last visited Jan. 16, 2020).

7. *Id.*

8. *Id.*

9. *See id.*; *see also* AnnaMaria Andriotis, *Cash, Plastic or Hand? Amazon Envisions Paying with a Wave*, WALL ST. J., https://www.wsj.com/articles/cash-plastic-or-hand-amazon-

In the United States, there are four states with statutes specifically providing safeguards for biometric data privacy, but with the development of biometric data technology resulting in increasing security risks, more states must enact legislation in order to fully protect citizens' biometric data.[10] Pennsylvania currently does not have a statute regulating the protection and use of its citizens' biometric data, nor do Pennsylvania's data breach notification laws—dictating how Pennsylvania businesses must notify affected Pennsylvania residents when a business experiences a harmful data breach[11]—provide protection for biometric data as personal information.[12] The lack of regulation is surprising given the sensitivity, permanence, and inherently unique features of biometric data.[13] It is imperative to protect Pennsylvania citizens' biometric identities from the risks that come with evolving biometric data practices.[14]

This article will first lay out the background of biometric data and the ways in which it is implemented.[15] Next, it will outline the current framework of U.S. state laws and the European Union's General Data Protection Regulation related to biometric data privacy.[16] Finally, this article will explain why Pennsylvania must enact a statute regulating the collection, retention, and use of the biometric data of its citizens.[17] This section will illuminate the need for state legislation over federal legislation and why a biometric data protection statute would best align with Pennsylvania's interests.[18] It will also discuss how Pennsylvania should approach statutory construction by incorporating a broad definition of "biometric data," affording biometric data protection as a fundamental right, and providing effective remedies for parties harmed by violations, including a private right of action and statutory penalties.[19]

---

envisions-paying-with-a-wave-11579352401 (Jan. 19, 2020, 11:58 AM) (discussing Amazon's vision of implementing the usage of palm prints for customer purchases).

10. *See* Blake Benson, *Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy*, 19 N.C. J.L. & TECH. ON. 161, 161 (2018) (advocating for a federal biometric privacy law).

11. *See generally* Breach of Personal Information Notification Act, 73 PA. STAT. AND CONS. STAT. ANN. §§ 2301–2329.

12. *Id.*

13. Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 KAN. L. REV. 637, 638 (2018).

14. *See infra* Section II.B.

15. *See infra* Section II.

16. *See infra* Section III.

17. *See infra* Section IV.

18. *See infra* Section IV.

19. *See infra* Section IV.

## II. BACKGROUND INFORMATION

### *A. What Is Biometric Data?*

In 2014, a group of hackers, suspected of working for the Chinese government, breached the United States Office of Personnel Management, stealing the personal data of an estimated 21 million Americans.[20] The stolen data contained the fingerprint information of 5.6 million people.[21] While federal experts concluded the ability to misuse the fingerprint data was limited in this event,[22] the potential for harm remains.[23] Increased implementation of biometric authentication systems, which compare biometric data to data that is already stored and confirmed in a database,[24] means more opportunities for hackers to use stolen biometric information to bypass or trick supposedly secure authentication systems.[25] Cybercriminals are rapidly finding new ways to profit and benefit from illegal activities, like identity theft, hacking of personal and corporate computer systems, and cyber stalking.[26] They can sell stolen biometric information to third parties, use it to board airplanes,[27] and to recreate fingerprints.[28] Through a tactic called spoofing, cyber hackers take photographs of latent fingerprints—from a surface like a drinking glass—and recreate them in a gelatin mold or artificial

---

20. *See* Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015, 2:00 PM), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.

21. *Id.* Many companies using biometrics do not store your actual fingerprints. *See* Anna Myers, *Can the U.S. Legal System Adapt to Biometric Technology?*, IAAP: PRIV. TECH (Aug. 12, 2016), https://iapp.org/news/a/can-the-u-s-legal-system-can-adapt-to-biometric-technology/. Instead, they convert fingerprint information into authentication codes, which are long numerical sequences that are hard to predict. *Id.* These authentication codes are then stored by the company as fingerprint information. *Id.*

22. Peterson, *supra* note 20.

23. *See generally* Jeremy Bergsman, *Biometrics Are Less Secure than Passwords—This Is Why*, BETANEWS, https://betanews.com/2016/08/24/unsafe-biometrics/ (last visited Oct. 30, 2019).

24. Dean Nicolls, *What Is Biometric Authentication?*, JUMIO (July 17, 2019), https://www.jumio.com/what-is-biometric-authentication/.

25. Marc Goodman, *You Can't Replace Your Fingerprints*, SLATE (Feb. 24, 2015, 10:05 AM), https://slate.com/technology/2015/02/future-crimes-excerpt-how-hackers-can-steal-fingerprints-and-more.html.

26. Danny Thakkar, *Fighting Crime and Tackling Terrorism with the Help of Biometric Technology*, BAYOMETRIC, https://www.bayometric.com/fighting-crime-with-the-help-of-biometric-technology/ (last visited Oct. 29, 2019).

27. Steve Symanovich, *Biometric Data Breach: Database Exposes Fingerprints, Facial Recognition Data of 1 Million People*, NORTONLIFELOCK, https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html (last visited Oct. 30, 2019).

28. Sayce, *supra* note 6.

silicon finger.[29] This technique is good enough to fool fingerprint scanners eighty percent of the time.[30] Even Play-Doh can be used to create fingerprint molds, which are able to trick ninety percent of fingerprint scanners.[31] Facial recognition systems, another common biometric security device, are also known to be vulnerable to cyber hacking when simply shown a photograph of an individual to unlock the individual's device.[32] Thus, when biometric information is collected and stored in a database, that information can be stolen and subsequently used for criminal activity.[33]

To fully appreciate the need for robust laws and regulations designed to prevent biometric data from falling into the wrong hands, it is important to have a basic understanding of what biometric data is and how it functions.[34] Although there is no universally accepted definition of biometrics,[35] it usually refers to either: "[m]easurable human biological and behavioral characteristics that can be used for identification," or "[t]he automated methods of recognizing or analyzing an individual based on those characteristics."[36] Simply stated, biometrics is the measurement of a person's physical being.[37] Biometric data generally refers to data that captures unique physical or behavioral characteristics as a means of verifying personal identity.[38] This data is derived from physiological and

29. *Id.*; *see also* Goodman, *supra* note 25.

30. Goodman, *supra* note 25.

31. *Id.*

32. Aside from traditional identity theft concerns, now any users of facial recognition programs must be concerned about other data weaponizations. *See* Sayce, *supra* note 6; *see also* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (Feb. 10, 2020) (discussing a groundbreaking facial recognition app, allowing a single picture taken of an individual to be matched with public photos across millions of websites, can make searching someone by face as easy as using Google to search a name: "There's always going to be a community of bad people who will misuse it[.]").

33. *See* Zimmerman, *supra* note 13, at 657.

34. *See generally Biometric Data and Data Protection Regulations (GDPR and CCPA)*, THALES, https://www.gemalto.com/govt/biometrics/biometric-data (Nov. 4, 2020).

35. Michael P. Daly et al., *Biometrics Litigation: An Evolving Landscape*, DRINKER BIDDLE & REATH LLP (Apr. 2, 2018), https://1.next.westlaw.com/w-001-8264?transitionType=Default&contextData=(sc.Default)&__lrTS=20171228100058671&firstPage=true&bhcp=1.

36. Peter A. Steinmeyer, *Expert Q&A on Biometrics in the Workplace: Recent Developments and Trends*, PRACTICAL L., https://www.ebglaw.com/content/uploads/2018/02/Sholinsky-Steinmeyer-Reuters-Expert-QA-Biometrics-February-2018.pdf (last visited Jan. 14, 2020).

37. Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. L. TODAY, May 2016, at 1.

38. *Biometrics*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/biometrics (last visited Oct. 28, 2019); *see also Biometrics*, HOMELAND SEC. (July 13, 2020), https://www.dhs.gov/biometrics.

behavioral identifiers.[39] Physiological identifiers include facial structure, retinal color and design, fingerprint readings, heat signatures, and DNA readings.[40] Behavioral identifiers include handwriting samples and signatures, voice recognition, and keyboard stroke and typing habits.[41] These identifiers allow for a person to be both authenticated, meaning to verify their identity, and identified, meaning to determine their identity.[42]

The character and value of biometric data can differ drastically from other, traditional forms of personal data. Biometric data is inherently permanent and unique to each individual, making it extremely sensitive information.[43] An individual's biometric information is exceedingly difficult to replace or change because it is unique to that person: "[I]t is very difficult, if not impossible, for any individual to disassociate oneself from one's biometric [information]."[44] Losing biometrics may not be a matter of replacement.[45] Passwords, credit cards, and even social security numbers can be replaced, but a person cannot get a new fingerprint.[46] Although choosing not to partake in biometric-facilitated transactions does not seem to be as drastic of a decision with few transactions involving the use of biometric data nowadays, biometric-facilitated transactions will one day become commonplace to consumers and retailers.[47] The personal effects of a breach could dissuade individuals from participating in such a transaction again in the future, which may lead to an overall chilling effect on the national economy.[48]

---

39. *See* Phil Ross, *Biometrics: A Developing Regulatory Landscape for a New Era of Technology*, ROBINSON & BRADSHAW (May 21, 2014), https://theprivacyreport.com/2014/05/21/biometrics-a-developing-regulatory-landscape-for-a-new-era-of-technology/.

40. *Id.*

41. *Id.*

42. *Biometrics: Definition, Trends, Use Cases, Laws and Latest News*, THALES, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (Dec. 4, 2020).

43. Benson, *supra* note 10, at 165.

44. Rigoberto Chinchilla, *Ethical and Social Consequences of Biometric Technologies*, AM. SOC'Y FOR ENG'G EDUC., 2012, at 1, 5–6.

45. *Id.* at 5.

46. Kaya Yurieff, *Why Are We Still Using Social Security Numbers as ID?*, CNN BUS. (Sept. 13, 2017, 8:40 AM), https://money.cnn.com/2017/09/13/technology/social-security-number-identification/index.html.

47. Recent studies show that mobile biometrics will "authenticate $2 trillion worth of in-store and remote mobile payment transactions annually by 2023." *See* Lynne Jeffery, *Biometrics and the Future of Payment Transactions*, BIOMETRICUPDATE.COM (Dec. 2, 2019), https://www.biometricupdate.com/201912/biometrics-and-the-future-of-payment-transactions. This not only demonstrates "a shift in consumer adoption of biometric authentication, but also rapid advancements in the technology being used to present these opportunities for biometric authenticated" transactions. *Id.*

48. Several studies indicate data security and privacy are essential in order to maintain customers: PwC reported 85% of consumers will not shop at a business if there are concerns about a business's security practices; Verizon reported that 69% of consumers would avoid a

### *B. Industries Implementing Biometric Data*

Biometric data is used currently in a variety of different applications, and that list of uses grows longer every day.[49] From opening up your smartphone with your fingerprint or facial recognition to unlocking your car to paying for groceries, biometric data is becoming a go-to method for many everyday tasks.[50] While biometrics are still predominately used for law enforcement purposes,[51] biometric data is also being deployed across the following industries: automotive, financial services and banking, healthcare, food and beverage, hospitality, retail, and education.[52]

In the automotive industry, biometrics are increasingly developed for security and driver safety features.[53] Devices such as iris or fingerprint scanners may become the standard security feature to lock, unlock, and start a vehicle, and automotive suppliers are leveraging biometric facial recognition and retina tracking to prevent driver distraction and fatigue.[54] In the financial services and banking industry, banking fraud is becoming more widespread.[55] Banks are adopting stricter identification protocols, including opting for fingerprint biometrics, to combat fraud and increase transaction security, as biometrics can help reduce fraudulent payments.[56] Various sectors of the healthcare industry are also using

---

company that had suffered a data breach and 29% of consumers surveyed would never visit that business again. *See* WORLDPAY ED. TEAM, *How the Consequences of a Data Breach Threaten Small Businesses*, FIS (July 10, 2019), https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses.

49. Catherine R. Tucciarello, *Rapid Increase in Biometric Data in Airports Raises Privacy Concerns*, JACKSON LEWIS (Mar. 1, 2019), https://www.workplaceprivacyreport.com/2019/03/articles/consumer-privacy/rapid-increase-in-biometric-data-in-airports-raises-privacy-concerns/.

50. *9 Industries Biometrics Technology Could Transform*, CB INSIGHTS (Dec. 12, 2019), https://www.cbinsights.com/research/biometrics-transforming-industries/.

51. *Id.* Biometrics have long been used by law enforcement with the use of DNA and fingerprints for reliable types of evidence in criminal cases. *Id.* There is a growing trend of law enforcement using facial recognition for identification purposes. *Id.* For example, facial recognition plays a big part in helping law enforcement to identify victims of sex trafficking between the US-Mexico border. *Id.*

52. *Id.*

53. "Other companies are developing in-vehicle biometrics for automotive security. For example, Porsche has partnered with edge computing software developer FogHorn to develop a multi-factor authentication prototype that uses real-time facial recognition plus additional authentication via smartphone, which allows drivers to enter into their cars without key fobs." *Id.* (noting the global market for automotive biometric identification is expected to reach $303M by 2024).

54. *Id.*

55. *Id.*

56. *Id.*; *see also* 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/.

measures, including facial recognition, and iris or fingerprint scanning, to advance telemedicine to make patient identification more accurate.[57] The food and beverage industries are increasingly using biometric technology to allow remote monitoring of employees and granting area access permissions, which minimizes cross-contamination.[58] In the hospitality industry, facial recognition is growing as a new way to provide better personalized services for customers.[59] Large retail companies are experimenting with biometric identification systems for payments and promotional targeting and the implementation of facial recognition to reduce theft.[60] Lastly, biometrics are applied to different aspects of education systems, including lunch programs, dorm access, security purposes, and preserving academic integrity for examinations.[61]

With each of these industries' investments in biometric data technology comes genuine security concerns.[62] Data breaches are growing more common.[63] In fact, more than half of U.S. businesses have experienced a cyberattack in the past year.[64] Just as companies must implement and update safeguards, legislatures and regulators must respond with legal efforts to protect biometric data privacy.[65]

## III. CURRENT BIOMETRIC DATA PROTECTION LAWS

As the use of biometric data becomes more prevalent, a handful of legislatures across the nation have taken note.[66] Despite the popularity of biometrics and the unique issues they pose, there is no single, comprehensive federal law in the United States regulating

57. *9 Industries Biometrics Technology Could Transform*, *supra* note 50.

58. *Id.* (noting Coca-Cola uses a biometric fingerprint system to track the activity of independent truck drivers entering certain canning sites).

59. *Id.*

60. *Id.* (noting Amazon is leading the way in terms of biometric payment systems for retail and is currently testing a scanner that uses computer vision and depth geometry to identify an individual's hand as a way to ring up a store purchase).

61. *Id.* (discussing facial recognition may be used to quickly identify any unauthorized presence within school grounds).

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

63. Joseph Cox, *Are Data Breaches Becoming More Common?*, VICE (July 28, 2016, 12:58 PM), https://www.vice.com/en_us/article/xygvgk/data-breaches-vigilante-pw.

64. According to CB Insights' Industry Analyst Consensus, the biometric technology industry is projected to be worth approximately $59 billion by 2025. *Cyber Attacks Infographic*, MUNICH RE (2017), https://www.munichre.com/HSB/cyber-risk-infographic/index.html.

65. *See* Kelly A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, 20 J. HIGH TECH. L. 229, 230 (2020).

66. *See* Wernick, *supra* note 56.

the collection and use of biometric information.[67] In the United States, four states, Illinois, Texas, Washington,[68] and California, have biometric data privacy statutes, and several others are debating enacting biometric privacy laws.[69] Additionally, the General Data Protection Regulation (GDPR), adopted by the European Union,[70] specifically addresses the protection of biometric data, representing a true international impact for data protection and privacy.[71] The increasing enactment of laws and regulations demonstrates a strong interest in protecting against threats and regulating the collection of biometric data.[72]

### *A. Illinois's Biometric Information Privacy Act (BIPA)*

In October 2008, Illinois enacted the first state law governing the collection, use, safeguarding, and storage of biometric data known as the Illinois Biometric Information Privacy Act (BIPA).[73] BIPA was enacted in response to the bankruptcy of a startup called Pay By Touch: a biometrics firm that enabled customers to make payments by connecting their financial accounts to their fingerprints.[74] Pay By Touch's bankruptcy and dissolution left customers with no information as to what would become of the biometric data and financial information they provided.[75] This event was the catalyst for the Illinois General Assembly to enact BIPA.[76] The Illinois General Assembly further reasoned that "[t]he use of biometrics is growing in the business and security screening sectors . . . ."[77] The General Assembly also reasoned that an affected individual "has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions" when their biometrics are compromised.[78] Thus, "[t]he public welfare, security,

67. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.
68. Wernick, *supra* note 56.
69. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.
70. *See generally* Council Directive 2016/679, 2016 O.J. (L 119) 1 (EU).
71. Council Directive 2016/679, art. 4, 2016 O.J. (L 119) 1, 34 (EU).
72. Chris Burt, *Biometrics Regulations Are Coming, Firm Warns as BIPA Lawsuits Pile Up*, BIOMETRICUPDATE.COM (Sept. 6, 2019), https://www.biometricupdate.com/201909/biometrics-regulations-are-coming-firm-warns-as-bipa-lawsuits-pile-up.
73. Ryan S. Higgins et al., *Biometric Privacy Update—Actual Harm Not Required*, MCDERMOTT WILL & EMERY (Feb. 7, 2019), https://www.mwe.com/insights/biometric-privacy-update-actual-harm-not-required/.
74. Justin O. Kay, *The Illinois Biometric Information Privacy Act*, DRINKER BIDDLE & REATH LLP, https://www.acc.com/sites/default/files/2019-02/Drinker-Biddle-2017-1-BIPA-Article-2.pdf (last visited Nov. 2, 2019).
75. *Id.*
76. *Id.*
77. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/5.
78. *Id.*

and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[79]

BIPA limits the private sector's collection, use, and retention of "biometric identifiers," such as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry.[80] The law also applies to "biometric information," which is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[81] The law requires private entities to provide individuals with notice, to obtain an individual's signed written release stating informed consent before collecting their biometric data,[82] to disclose both the lawful purpose for the collection of data and the amount of time the data will be kept, and to destroy the information within a certain timeframe.[83] Furthermore, BIPA prohibits private entities from using a consumer's biometric information for profit and requires written policies concerning biometric data retention and destruction that are accessible to the public.[84]

Unlike data privacy statutes in other states, BIPA creates a private right of action against private entities that fail to satisfy BIPA's requirements with respect to the collection and use of biometric information.[85] This means that individuals, either on their own or via class actions, may seek enforcement through civil litigation claiming monetary relief.[86] BIPA also entitles a prevailing party to the following statutory damages: for each negligent violation of BIPA equal to the greater of $1,000 or actual damages, or for

79. *Id.*

80. 740 ILL. COMP. STAT. ANN. 14/10.

81. *Id.*

82. *See* Carley Daye Andrews et al., *Litigation Under Illinois Biometric Information Privacy Act Highlights Biometric Data Risks*, K&L GATES (Nov. 7, 2017), http://www.klgates.com/litigation-under-illinois-biometric-information-privacy-act-highlights-biometric-data-risks-11-07-2017/.

83. 740 ILL. COMP. STAT. ANN. 14/15.

84. *Id.* BIPA explicitly prohibits private entities from selling, leasing, trading, or "otherwise profit[ing] from" an individual's biometric data. Michael Bahar et al., *Biometrics Beware—Compliance and the Biometric Information Privacy Act*, JD SUPRA (Apr. 12, 2019), https://www.jdsupra.com/legalnews/biometrics-beware-compliance-and-the-66757/ (alteration in original). There are currently no BIPA class actions based on this provision, which raises questions regarding how courts will interpret the phrase "otherwise profit." *Id.*

85. Ronald J. Hedges & Gail L. Gottehrer, *Beyond HIPAA: Examining Data Privacy Laws at the State Level*, J. AHIMA (May 1, 2019, 12:01 AM), https://journal.ahima.org/beyond-hipaa-examining-data-privacy-laws-at-the-state-level/.

86. Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, K&L GATES (Mar. 25, 2019), http://www.klgates.com/the-biometric-bandwagon-rolls-on-biometric-legislation-proposed-across-the-united-states-03-25-2019/.

each intentional or reckless violation of BIPA the greater of $5,000 or actual damages.[87] Additionally, in January 2019, the Illinois Supreme Court held that plaintiffs need not "plead and prove that they sustained some actual injury or damage beyond infringement of the rights afforded them under the [BIPA]" in order to have a cause of action.[88] BIPA has been said to be the "the archetype . . . of biometric privacy law,"[89] and it appears to be one of the biometric data protection statutes to emulate.[90]

### *B. Texas's Capture or Use of Biometric Identifier (CUBI) and Washington's House Bill 1493 (H.B. 1493)*

Shortly after Illinois passed BIPA, Texas enacted a biometric data protection statute in 2009.[91] The Capture or Use of Biometric Identifier Act (CUBI) is similar to BIPA in that it contains similar substantive provisions to that of BIPA, particularly regarding prohibiting private entities from collecting biometric information before giving notice and obtaining an individual's consent,[92] making profits off of the sale of biometric data, and requiring certain security and retention measures.[93] However, CUBI differs from BIPA in that it does not create a private right of action, but instead permits the Texas Attorney General to bring a civil action and provides for a penalty cap of $25,000 per violation.[94] The CUBI also defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[95]

Washington became the third state to enact a biometric privacy statute in 2017 with House Bill 1493 (H.B. 1493), which is similar to CUBI.[96] The Annotated Revised Code of Washington defines a

87. Claypoole & Stoll, *supra* note 37, at 2.

88. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019); *see also* Molly K. McGinley et al., *"No Harm, Still Foul": Actual Harm Not Required for Plaintiffs Under Illinois Biometric Privacy Act*, NAT'L L. REV. (Jan. 26, 2019), https://www.natlawreview.com/article/no-harm-still-foul-actual-harm-not-required-plaintiffs-under-illinois-biometric.

89. Jane Bambauer, *Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal*, PROGRAM ON ECON. AND PRIV., https://pep.gmu.edu/wp-content/uploads/sites/28/2017/06/Biometric-Privacy-Laws-FINAL_really_6.20-.pdf (last visited Dec. 19, 2020).

90. *See* Claypoole & Stoll, *supra* note 37.

91. *See generally* Capture or Use of Biometric Identifier, TEX. BUS. & COM. CODE ANN. § 503.001.

92. TEX. BUS. & COM. CODE ANN. § 503.001(b)–(c); *see also* Claypoole & Stoll, *supra* note 37, at 2.

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

94. *Id.* § 503.001(d).

95. *Id.* § 503.001(a).

96. *See generally* H.B. 1493, 2017 Leg., Reg. Sess. (Wash. 2017).

"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 or characteristics that is used to identify a specific individual."[97] H.B. 1493 broadly regulates the collection, retention, and use of "biometric identifiers," and like CUBI, permits the state's Attorney General to bring a civil action with a penalty cap of $25,000.[98]

### *C. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)*

The California Consumer Privacy Act (CCPA) of 2018 similarly provides protections for consumer data, including biometric data.[99] The CCPA recently went into effect on January 1, 2020.[100] It defines "biometric information" as "an individual's physiological, biological, or behavioral characteristics, including an individual's [DNA], that can be used, singly or in combination with each other or with identifying data, to establish individual identity."[101] The CCPA establishes a narrow private right of action for certain data breaches involving a subset of personal information, and consumers may seek actual damages or statutory damages ranging from $100 to $750 per intentional violation.[102] The act also provides a maximum penalty of $7,500 for intentional violations, while other violations lacking intent remain subject to a preset fine of $2,500.[103] One hotly contested part of the CCPA is its "notice and cure" provision, which provides an avenue for a company to avoid individual statutory damages if a company cures its violations within thirty days.[104] This provision ultimately compels a company to implement and maintain reasonable security procedures and practices.[105]

---

97. WASH. REV. CODE ANN. § 19.375.010.
98. *Id.* § 19.86.140.
99. *See generally* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.
100. *Id.*
101. *See id.* § 1798.140(b) (stating "[b]iometric 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 can contain identifying information.").
102. *Id.* § 1798.150; *see also* Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKERHOSTETLER LLP, https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf (last visited Nov. 1, 2019).
103. CAL. CIV. CODE § 1798.155.
104. *Id.* § 1798.150(b).
105. *Id.*

Most notably, the CCPA empowers California consumers with fundamental privacy rights to control their own personal information,[106] providing many similar protections as the European Union's GDPR.[107] The CCPA follows in the footsteps of the GDPR by allowing individuals to have greater control over their personal data.[108] The CCPA offers California consumers new statutory rights, including the Consumer Right to Delete, Consumer Opt-Out from Sale of Personal Information, Consumer Opt-In for the Sale of Personal Information of Minors, and Non-Discrimination for Exercise of Consumer Rights.[109] These provisions in the CCPA afford consumers with individual rights to learn what personal information covered businesses have collected, sold and disclosed, opportunities to opt-out of the sale of their personal information, and the unique protection from discrimination in the form of reduced service or functionality for exercising those rights.[110] With strong similarities to the GDPR, the CCPA is frequently presented as a model for future legal framework of U.S. data privacy law.[111]

Although the CCPA currently provides comprehensive data protections for its citizens, recent events demonstrate that privacy regulation in the state of California will not stop with the CCPA.[112] On November 3, 2020, Californians voted to approve a ballot initiative known as Proposition 24, which enacted the California Privacy Rights Act (CPRA).[113] Taking effect on January 1, 2023, the CPRA

106. *See* Xavier Becerra, *California Consumer Privacy Act (CCPA)*, CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa (last visited Dec. 19, 2020).

107. CAL. CIV. CODE §§ 1798.100–1798.199. The CCPA provides the following rights to consumers: to know all data collected on a consumer by a business, twice a year, free of charge; to say no to the sale of a consumer's information; to delete the data posted; to sue companies who collect their data, where that data was stolen or disclosed pursuant to an unauthorized data breach, if the company was careless or negligent about how it protected one's data; not to be discriminated against for telling a company not to sell one's personal information; to be informed of what categories of data will be collected about one prior to its collection or at point of collection, and of any charges made to this collection; mandated opt-in before sale of children's information; to know the categories of third parties with whom your data is shared; to know the business or commercial purpose of collecting one's information. *See infra* Section III.D.

108. Palmer, *supra* note 5.

109. John Stephens, *California Consumer Privacy Act*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

110. *Id.*

111. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.

112. Cynthia Cole et al., *Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now*, BLOOMBERG L. (Nov. 16, 2020, 4:00 AM), https://news.bloomberglaw.com/privacy-and-data-security/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now.

113. The California Privacy Rights Act of 2020, Cal. Proposition 24 (2020), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

is not intended to replace the CCPA; rather, the CPRA incorporates the CCPA and includes a number of amendments and modifications to the CCPA.[114] The CPRA amends and expands upon the CCPA by creating additional consumer rights, modifying existing CCPA rights, establishing a new privacy enforcement agency, and mandating a new subcategory of consumer personal information known as "sensitive personal information."[115] Biometric data is included as an identifier that qualifies as sensitive personal information.[116] While the CCPA implicitly includes the regulation of sensitive personal information in broader terms, the CPRA imposes distinct requirements and restrictions on regulating sensitive personal information, including disclosure requirements, opt-out requirements for use and disclosure, opt-in consent standard for use and disclosure, and purpose limitation requirements.[117] Ultimately, the enactment of the CPRA represents a significant shift in the U.S. privacy landscape and will likely energize efforts to pass other data privacy acts throughout the nation.[118]

### *D. General Data Protection Regulation (GDPR)*

Aside from the biometric data protection laws in the United States, the General Data Protection Regulation serves as an exemplary international standard for data protection.[119] The GDPR was passed in April of 2016 and went into effect on May 25, 2018.[120] Not only does the GDPR apply to organizations located within the European Union, but it also applies to all companies, anywhere in the world, processing and holding the personal data of those that reside in the European Union.[121] It defines "biometric data" as "personal data resulting from specific technical processing relating to the physical, physiological or [behavioral] characteristics of a natural person, which allow or confirm the unique identification of that

114. Matthew A. Diaz & Kurt R. Hunt, *California Approves the CPRA, a Major Shift in U.S. Privacy Regulation*, NAT'L L. REV. (Nov. 17, 2020), https://www.natlawreview.com/article/california-approves-cpra-major-shift-us-privacy-regulation.

115. Cole et al., *supra* note 112.

116. *Id.*

117. Brandon P. Reilly & Scott T. Lashway, *The California Privacy Rights Act Has Passed: What's in It?*, MANATT (Nov. 11, 2020), https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed.

118. Diaz & Hunt, *supra* note 114.

119. *See generally* Laurent Barthelemy, *One Year on, EU's GDPR Sets Global Standard for Data Protection*, PHYS.ORG (May 24, 2019), https://phys.org/news/2019-05-year-eu-gdpr-global-standard.html.

120. Palmer, *supra* note 5.

121. Ben Wolford, *Does the GDPR Apply to Companies Outside of the EU?*, GDPR.EU, https://gdpr.eu/companies-outside-of-europe/ (last visited Feb. 16, 2020).

natural person, such as facial images or dactyloscopic [fingerprint] data."[122] The GDPR also establishes a private right of action for material or non-material damages caused by a data controller or data processors breach.[123] Material damage involves actual damage that is quantifiable, while non-material damage involves any damage that is not financial, such as pain and suffering.[124] The GDPR imposes penalties of up to four percent of an organization's annual global turnover, or a company's total revenues,[125] or twenty million euros, whichever is greater.[126]

Most notably, the GDPR affords the following rights to its citizens: right to breach notification; right to access; right to be forgotten; right to data portability; right to know whether or not personal data is being processed, where, and for what purpose; a free copy of personal data in electronic format; the right to have the data controller erase his or her data, cease further dissemination of the data, and potentially have third parties halt processing of the data; the right to obtain personal data in a commonly used and machine readable format; and the right to transfer that data to another controller.[127]

Not only has the GDPR enhanced data protection for citizens in the European Union, but it has become globally influential, being referred to as the new "gold-standard" for the protection of data worldwide.[128] At its core, the GDPR is designed to give citizens of the European Union more control over their personal data.[129] Countries and regions around the world appear to be taking cues from

122. *See* Council Directive 2016/679, *supra* note 70, at art. 4.

123. *Id.* at art. 82.

124. Deirdre Kilroy, *Data Protection Litigation—An Irish Perspective*, MATHESON (Sept. 12, 2018), https://www.matheson.com/news-and-insights/article/data-protection-litigation-an-irish-perspective.

125. Adam Hayes, *Overall Turnover*, INVESTOPEDIA (July 2, 2019), https://www.investopedia.com/terms/o/overall-turnover.asp.

126. *See generally* Council Directive 2016/679, *supra* note 70, at art. 12–23.

127. *See generally id.*

128. Maeva Kpadonou, *With the GDPR, Europe Shows the World the Way*, LEADERS LEAGUE (Nov. 4, 2019), https://www.leadersleague.com/en/news/with-the-gdpr-europe-shows-the-world-the-way.

129. Some scholars argue this European value of privacy is largely due to Europe's past experiences, particularly with the Nazis in the twentieth century, with fascism and communism. *See* David Meyer, *Opinion: How Europe Is Better at Protecting Data than the U.S.—and What the Stasi and Nazis Have to Do with It*, MKT. WATCH (Mar. 21, 2018, 1:34 PM), https://www.marketwatch.com/story/why-europe-does-a-better-job-of-protecting-online-privacy-than-the-us-does-2018-03-20; *see also* Jeffrey Toobin, *The Solace of Oblivion: In Europe, the Right to Be Forgotten Trumps the Internet*, NEW YORKER (Sept. 22, 2014), https://www.newyorker.com/magazine/2014/09/29/solace-oblivion. *But see* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004) (stating scholars have alternatively theorized that European Union views privacy as an aspect of dignity based on ancient European practices for defending reputation).

the GDPR by introducing or modifying data protection legislation, as demonstrated with the enactment of the CCPA.[130] The GDPR is an exemplary demonstration of the importance of building a foundation of trust in a digital future, thus ensuring citizens that they are in control of their personal information, and their information is always protected.[131]

## IV. ANALYSIS: IMPLEMENTING BIOMETRIC DATA PROTECTIONS IN PENNSYLVANIA

### *A. State Legislation over Federal Legislation*

Although scholars argue that enacting federal legislation would be a more appropriate solution to solve biometric privacy concerns, biometric data legislation will likely be more successful at the state level.[132] Companies conducting business across multiple states allege that compliance with biometric data protections would be easier if there was one uniform standard to follow.[133] However, there are issues regarding the lengthy deliberation process of creating federal legislation.[134] Congress passes far fewer bills, both as a percentage of those introduced and as a raw number, than state legislatures.[135] Legislation moves faster and is passed with greater frequency at the state level.[136] State legislatures pass about a quarter of the bills that are offered.[137] This allows for states to act as "laboratories of democracy," serving as proper testing grounds for biometric data protection laws and ultimately influencing an appropriate federal law protecting citizens' biometric data nationwide.[138]

---

130. Whitman, *supra* note 129; Meyer, *supra* note 129; Toobin, *supra* note 129.

131. Whitman, *supra* note 129; Meyer, *supra* note 129; Toobin, *supra* note 129.

132. *See generally* Daniel C. Vock, *State Labs: Congress Can Learn a Lot from State Legislatures*, GOVERNING (Sept. 2019), https://www.governing.com/topics/politics/gov-state-labs.html.

133. Fiona Q. Nguyen, Article, *The Standard for Biometric Data Protection*, 7 J.L. & CYBER WARFARE 61, 71 (2018).

134. Vock, *supra* note 132 (noting that during the last Congress, members introduced nearly 11,200 bills over two years, and only 416 of them became law, and even including those, less than four percent of bills introduced became law).

135. *Id.*

136. *State Legislatures vs. Congress: Which Is More Productive?*, QUORUM, https://www.quorum.us/data-driven-insights/state-legislatures-versus-congress-which-is-more-productive/176/ (last visited Nov. 2, 2019) ("[S]tate legislatures introduce [twenty-three] times more bills than Congress does, totaling an average 128,145 bills per year and 3.1 million words per day in session.").

137. Vock, *supra* note 132.

138. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("[A] single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

Rather than facing a Congressional gridlock and continue to delay the enactment of an ideal uniform federal standard, enacting biometric data protections through state legislation is the best option for quickly and efficiently regulating this information.[139] As technology continues to develop, consumers' privacy interests continue to be urgent and outweigh the arguments against biometric legislation, and waiting for Congress to draft the perfect uniform federal biometric data protection law.[140] Protections for Pennsylvania citizens' biometric information could be implemented more quickly and efficiently if the Pennsylvania legislature enacted its own statute.[141]

### *B. Why Pennsylvania?*

As more states propose and enact legislation protecting the collection, retention, and use of biometric data,[142] Pennsylvania must consider these proposals and enactments and its own biometric privacy law to encourage similar standards of compliance for the protection of its own citizens, consumers, and companies.[143] There is currently no statute that specifically protects citizens' biometric data in Pennsylvania, and Pennsylvania's data breach notification law also does not contain "biometric information" under its protected "personal information."[144] Although it would improve biometric data privacy protections to an extent, it is not enough for Pennsylvania to simply amend its data security breach notification laws to include "biometric data" as a type of "personal information."[145] A comprehensive statute will provide Pennsylvania consumers more protection because, like the other biometric data protection statutes in place, it will recognize that biometric information is distinct from other types of personal information and

139. *See generally State Legislatures vs. Congress*, *supra* note 136.

140. *See* Carra Pope, Note and Comment, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 799 (2018).

141. *See generally State Legislatures vs. Congress*, *supra* note 136.

142. *See* McGinley, *supra* note 86 (Arizona, Florida, and Massachusetts are the latest states to propose legislation addressing biometric information protections).

143. *See generally* Nguyen, *supra* note 133.

144. *See* Breach of Personal Information Notification Act, 73 PA. STAT. AND CONS. STAT. ANN. § 2302 (defining "personal information" as "(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number; (ii) Driver's license number or a State identification card number issued in lieu of a driver's license; (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.").

145. *See generally id.*

acknowledge that the potential harms are not limited to data security breaches.[146]

There are several features specific to the state of Pennsylvania which make enacting state legislation the best choice for furthering biometric data protections. One of the most significant factors to consider for enacting a statute for biometric data protection is Pennsylvania's economy.[147] With two major metropolitan areas facilitating a tremendous amount of business throughout the state, Pennsylvania has the sixth largest economy in the United States by GDP.[148] If Pennsylvania does not protect these consumers, Pennsylvania puts its consumers at a greater risk as biometric data becomes increasingly relevant in various industries.[149] Furthermore, if Pennsylvania does not provide guidelines for companies to protect consumers' biometric data, it would ultimately fail its citizens by not protecting their biometric data.[150] Legislators all across the nation are making data privacy a top priority, resulting in a domino effect as the number of laws proposed for proactive and reactive data security measures are spiking.[151] If Pennsylvania neglects to pass this legislation, it would disturb this domino effect and would not influence other states to implement similar protections.[152] This ultimately discourages the expansion of biometric data protection laws throughout the nation.[153] Thus, it is logical for the Pennsylvania General Assembly to implement a statute to establish a sense of trust in consumers that their sensitive data will be protected, which allows consumers to feel more comfortable turning their data over, and in turn, allows for a more prosperous economy.[154]

---

146. Zimmerman, *supra* note 13, at 648.

147. *See Gross Domestic Product by State, 2nd Quarter 2020*, BUREAU OF ECON. ANALYSIS, (Oct. 2, 2020, 8:30 AM), https://www.bea.gov/sites/default/files/2020-10/qgdpstate1020_0.pdf.

148. *Id.*

149. *See infra* Section IV.B.

150. *See* NAT'L RSCH. COUNCIL, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 85 (Joseph N. Pato & Lynette I. Millett eds., 2010).

151. *See* Mark S. Goldstein et al., *The Sword Behind the SHIELD: Implications of New York's Expanded Data Security Law for Employers and the Broader Biometric Landscape*, REED SMITH (Oct. 23, 2019), https://www.reedsmith.com/en/perspectives/2019/10/the-sword-behind-the-shield.

152. The CCPA's impact on privacy regulation across the United States is discussed as starting a new wave of privacy focused standards in the U.S. *See generally* Lindsey O'Donnell, *California's Domino Effect on U.S. Privacy Regulation*, THREATPOST (Nov. 14, 2019, 10:32 AM), https://threatpost.com/ccpas-domino-effect-us-privacy-regulation/150246/.

153. *See* Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

154. *See generally* Sam Saltis, *GDPR Fines: Everything You Need to Know*, CORE DNA (Nov. 5, 2020), https://www.coredna.com/blogs/gdpr-fines.

Additionally, Pennsylvania's Constitution demonstrates strong values placed on individual privacy rights and consumer protection.[155] The Pennsylvania Supreme Court has interpreted both Article 1, Section 1 and Article 1, Section 8 of the Pennsylvania Constitution as being tied to the implicit right to privacy in the Commonwealth of Pennsylvania.[156] In fact, the Commonwealth of Pennsylvania has long embodied a commitment to the protection of individual privacy.[157] Pennsylvania courts have regularly stated that Pennsylvania's right to privacy encompasses freedom from disclosure of personal information.[158] With these privacy interests embedded in the provisions of the Pennsylvania Constitution, the enactment of a statute protecting biometric data privacy would align properly with interests that the Commonwealth of Pennsylvania seeks to continuously protect.[159]

### *C. Affording Privacy Rights*

In order to fully protect its citizens' biometric information, the Pennsylvania legislature must consider affording statutory rights to consumers in its biometric privacy provisions.[160] The inclusion of statutory rights with biometric data protections is demonstrated in the GDPR, BIPA, and CCPA.[161] The rights afforded under these provisions must be considered in the drafting of Pennsylvania's biometric data protection statute: right to breach notification; right to access; right to be forgotten; right to data portability; right to know whether or not personal data is being processed, where, and for what purpose; the right to have the data controller erase his or her data, cease further dissemination of the data, and potentially have third parties halt processing of the data; the right to obtain

155. PA. CONST. art. I, § 1, 8.

156. *See, e.g.*, Commonwealth v. Murray, 223 A.2d 102, 109–10 (Pa. 1966) (Musmanno, J.) (plurality opinion) (stating that the right to privacy is rooted in the Article I, Section I protection of "inherent and indefeasible rights" and in Article I, Section 8); *see* Pa. State Educ. Ass'n v. Commonwealth, 148 A.3d 142, 151 (Pa. 2016); Commonwealth v. Russo, 934 A.2d 1199, 1200 (Pa. 2007); Commonwealth v. Edmunds, 586 A.2d 887, 901 (Pa. 1991).

157. Seth F. Kreimer, *The Right to Privacy in the Pennsylvania Constitution*, 3 WIDENER J. PUB. L. 77, 82 (1993).

158. *Id.* at 102; *see* Denoncourt v. Pennsylvania State Ethics Comm'n, 470 A.2d 945, 948 (Pa. 1983); *see also In re* June 1979 Allegheny Cnty. Investigating Grand Jury, 415 A.2d 73, 77 (Pa. 1980); Fischer v. Commonwealth, Dep't of Pub. Welfare, 482 A.2d 1148, 1159 (Pa. Commw. Ct. 1984) (en banc).

159. *See generally Denoncourt*, 470 A.2d at 948. *See also In re June 1979 Allegheny Cnty. Investigating Grand Jury*, 415 A.2d at 77; *Fischer*, 482 A.2d at 1159.

160. *See generally* CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; Council Directive 2016/679, *supra* note 70, at art. 12–23.

161. CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; Council Directive 2016/679, *supra* note 70, at art. 12–23.

personal data in a common use and machine readable format; and the right to transfer that data to another controller.[162]

Each of the rights afforded under these biometric data privacy laws highlight different protections and needs.[163] The right to be informed, or the right to know whether or not data is being processed, highlights the need for transparency from companies regarding how these companies process an individual's data.[164] The right to be forgotten, or the right to erasure, gives individuals the right to demand that their data be removed or deleted from a database, which obligates companies to erase all data about the individual, unless it must be stored for a legal purpose.[165] The right to restrict processing, or to have third parties halt processing of the data, gives individuals the rights to block or suppress the processing of personal data.[166] The right to data portability ensures that individuals can reuse their personal data for their own purposes across different services.[167] Considering what each of these rights provide for individuals, incorporating statutory rights in Pennsylvania's biometric data protection statute would allow consumers to have control over the collection, aggregation, and retention of their biometric data and shift the burden over to companies to justify their use of and protection of this data.[168]

### *D. Defining "Biometric Data"*

When drafting a biometric data protection statute, the Pennsylvania legislature must construct a definition of "biometric data" that fully protects each aspect of its consumers' biometric information and that makes it simple for other out-of-state companies to abide by.[169] Defining "biometric data" too narrowly would likely fail to encompass certain classifications of biometric data that should rightfully be protected.[170] The legislature must consider a

162. Council Directive 2016/679, *supra* note 70, at art. 12–23.

163. *See generally Consumer Rights and GDPR*, LEADDESK, https://leaddesk.com/gdpr-consumer-rights-2/ (last visited Dec. 19, 2020).

164. *Id.*

165. *Id.*

166. *Id.* Under the GDPR, processing covers a range of operations performed on data, including "the collection, recording, [organization], structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data." *What Constitutes Data Processing?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en (last visited Feb. 14, 2020).

167. *Consumer Rights and GDPR*, *supra* note 163.

168. *See generally id.*

169. *See* Zimmerman, *supra* note 13, at 666.

170. *Id.*

definition for "biometric data" that not only encapsulates as many biological characteristics as possible, but one that also is in line with technological changes in order for the law to keep up with ever-advancing technologies.[171] However, the legislature should consider balancing this broad definition by including a provision to prevent the conversion of biometric data into other formats, similar to the provision included in BIPA: "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[172] This provision will prevent organizations from circumventing the law and converting biometric identifiers into other formats.[173]

Both the GDPR and the CCPA's definitions of "biometric data" and "biometric information," respectively, allow for all potential forms of biometric information to be protected.[174] The GPDR's inclusion of "physical, physiological, and behavioral characteristics" as biometric identifiers appears to be an implicit acknowledgement that biometric technology is relatively nascent and will continue to evolve beyond our current understanding.[175] The CCPA's definition of "biometric information" extends to unique biological characteristics and the data generated by measuring them.[176] The CCPA's definition includes elements of the GDPR's definition of special categories of data, but it broadly incorporates the idea that biometric data "can be used, singly or in combination with each other or with other identifying data, to establish individual identity."[177] With both the GDPR and CCPA's inclusive definitions serving as model laws, the Pennsylvania legislature should also set out a broad definition of "biometric data," using a technology-neutral definition focusing on the *type* of data that is collected by biometric technologies, ultimately allowing the statute to provide a flexible standard that can be applied to new and evolving technologies in the future.[178]

---

171. *Id.*
172. 740 ILL. COMP. STAT. ANN. 14/10.
173. QUINN EMANUEL URQUHART & SULLIVAN, LLP, *June 2019: The Rise of Biometric Laws and Litigation*, JD SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/june-2019-the-rise-of-biometrics-laws-82168/.
174. *See* CAL. CIV. CODE §§ 1798.100–1798.199; Council Directive 2016/679, *supra* note 70, at art. 4.
175. Danny Ross, *Processing Biometric Data? Be Careful, Under the GDPR*, INT'L ASS'N OF PRIV. PROF'LS (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/.
176. *See* Jonathan (Yoni) Schenker & Craig A. Newman, *Part I: A Closer Look at California's New Privacy Regime: The Definition of "Personal Information,"* PATTERSON BELKNAP (Apr. 9, 2019), https://www.pbwt.com/data-security-law-blog/part-i-a-closer-look-at-californias-new-privacy-regime-the-definition-of-personal-information.
177. *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, *supra* note 34.
178. Zimmerman, *supra* note 13, at 668.

### *E. Private Right of Action*

Like the GDPR, BIPA, and CCPA, Pennsylvania must offer a mechanism by which parties in violation of the law can be held accountable.[179] The most direct approach to offer effective recourse is for Pennsylvania to include a private right of action in its biometric data protection statute.[180] Offering a private right of action will allow Pennsylvania citizens to enforce protections of their rights and get equal consideration for their claims without relying on the Attorney General.[181] Attorney General offices have limited time and resources to pursue every claim, and cases involving delicate biometric information should not be selectively pursued.[182] Although some scholars argue that adding a private right of action creates a flood of litigation, a clear and comprehensive law balancing privacy and business interests will minimize litigation, and it is a small price to pay for strong protections of Pennsylvanian's biometric information.[183] Creating a private right of action would ultimately provide data breach victims with a right to hold violators accountable.[184]

On the contrary, a statute that does not provide a private right of action for a biometric data breach increases the risks involved in privately suing a compromised entity, leaving the injured party to rely on legal theories independent of specific laws.[185] BIPA's inclusion of a private right of action is one of the most imperative aspects of the statute, as it was created in the aftermath of a private entity dissolving, leaving questions for consumers about what would become of their sensitive biometric data.[186] With biometric authentication technology being used more often by the average adult today, many Americans believe they have lost control of their data and are unsure how to get it back under their control.[187] This is not entirely surprising considering how few data breach victims are able to

179. *See generally* CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; Council Directive 2016/679, *supra* note 70, at art. 82.

180. Michael A. Rivera, Note, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 571, 595 (2019).

181. Benson, *supra* note 10, at 191.

182. *Id.*

183. *Id.*

184. Rivera, *supra* note 180, at 595.

185. *Id.* at 582–83.

186. *See* Kay, *supra* note 74.

187. *See* Mary Louise Kelly, *Most Americans Feel They've Lost Control of Their Online Data*, NPR (Apr. 10, 2018, 7:02 PM), https://www.npr.org/2018/04/10/601148172/most-americans-feel-theyve-lost-control-control-of-their-online-data.

successfully hold private entities legally accountable for failure to protect this sensitive biometric data.[188]

A private right of action also provides a mechanism in which harmed consumers can avoid the class certification challenges present in data breach class action suits.[189] "The private right [of action] can also provide an alternate means to bring suit against private entities with forced arbitration clauses [which] specifically prohibit class action suits."[190] Other jurisdictions have offered a private right of action, demonstrating that it is a workable option for legal recourse.[191] For example, there is little to suggest that Illinois suits brought through this private right of action offered in BIPA have become unduly burdensome on Illinois businesses or courts.[192] A private right of action is an element that ultimately prioritizes the safety of consumer biometric data and empowers consumers to hold private entities accountable.[193] Therefore, a private right of action should be incorporated in Pennsylvania's biometric data protection statute in order to provide proper remedies for its citizens who have been harmed by violators.[194]

### *F. Penalties for Statutory Violations*

Independent of this private right of action, Pennsylvania should consider imposing monetary civil penalties for when its biometric data protection statute is violated.[195] Imposing high penalties like the GDPR—up to four percent of an organization's annual global turnover or twenty million euros, whichever is greater—will deter violation of the statute.[196] Businesses argue the fines outlined under the GDPR are unreasonably high and could extinguish companies' operations if there were a data breach or violation of the standard.[197] However, with over half of businesses experiencing cyberattacks in the United States, legislatures must implement higher standards of protection to combat cyber hackers and reduce the

188. Rivera, *supra* note 180, at 598.
189. *Id.*
190. *Id.*
191. *Id.* at 599.
192. *Id.*
193. *Id.* at 610.
194. *See* Benson, *supra* note 10, at 166.
195. *See generally* CAL. CIV. CODE §§ 1798.150–1798.155; 740 ILL. COMP. STAT. ANN. 14/20; TEX. BUS. & COM. CODE ANN. § 503.001(d); WASH. REV. CODE ANN. § 19.86.140; Council Directive 2016/679, *supra* note 70, at art 83.
196. Nguyen, *supra* note 133, at 81.
197. *See If the Data Breach Doesn't Kill Your Business, the Fine Might*, TRIPWIRE (Apr. 1, 2019), https://www.tripwire.com/state-of-security/security-data-protection/data-breach-fine/.

amount of cyberattacks.[198] Higher penalties can motivate data collectors and companies to invest in increased security measures, which will save companies from the damage of fines, lawsuits, and damage to their reputations.[199] If companies are held to higher standards, this encourages greater compliance with biometric data protection standards and overall security of consumers' sensitive biometric data.[200] Pennsylvania must impose penalties under its biometric data protection statute in order to effectively protect both themselves and their customers.[201]

To ensure that businesses are not financially extinguished by penalties, Pennsylvania can consider implementing a "notice and cure" provision for noticed violations.[202] Under its "notice and cure" provision, the CCPA grants businesses a thirty-day cure period, in the event that a cure is possible, to avoid statutory damages or class-wide damages.[203] A private plaintiff, one who is affected by an unauthorized disclosure or theft of personal information, must provide a business written notice within thirty days identifying the specific provisions of this title and the consumer alleges have been or are being violated prior to filing their lawsuit.[204] The notion of cure is not defined in the CCPA, but it has the flexibility to be interpreted narrowly, meaning a specific incident is cured to the extent possible at the time the business receives notice of the violation, or broadly, meaning the business's reasonable security procedures and practices must be remedied as a whole.[205] While the notice and cure provision will not affect lawsuits for actual damages, it provides an avenue for companies to continue operating and to cure issues relating to data incidents, as well as helping to ensure consumers that companies are compelled to keep security procedures and practices effective and up to date.[206]

Although the CCPA's "notice and cure" provision provides measures to protect both businesses and consumers when violations occur, it also raises many questions as to what constitutes a proper

198. *Cyber Attacks Infographic*, *supra* note 64.
199. Saltis, *supra* note 154.
200. *See* Nguyen, *supra* note 133, at 81.
201. *See* Saltis, *supra* note 154.
202. *See generally* CAL. CIV. CODE § 1798.150.
203. *Id.*
204. James M. Perez & Sheri Porath Rockwell, *Navigating the CCPA's 'Notice and Cure' Provision*, BLOOMBERG L., https://www.sidley.com/-/media/publications/bloomberg-law_navigating-the-ccpas-notice-and-cure-provision.pdf (last visited Jan. 18, 2020).
205. COOLEY LLP, *United States: CCPA FAQs Part 3: Litigation, Regulatory Actions and Liability*, MONDAQ (Oct. 7, 2019), http://www.mondaq.com/unitedstates/x/851552/Data+Protection+Privacy/CCPA+FAQs+Part+3+Litigation+Regulatory+Actions+and+Liability.
206. *See generally* Perez & Rockwell, *supra* note 204.

"cure."[207] The Pennsylvania legislature must draft this provision with clearer standards on what companies must do to cure purported violations.[208] A clearer definition for a "cure" should make clear that the cure must relate to the company's violation of its duty to maintain and provide reasonable security procedures and practices.[209] This would not only avoid confusion in the courts, but it would also allow businesses to consider possible responses in cases of violations and ways to further enhance biometric data security practices, as these decisions must be made quickly within a thirty-day time frame.[210] To ensure the explanation of an appropriate "cure" is not too narrow, the Pennsylvania legislature should consider including that the appropriate "cure" should be informed by the circumstances of each breach and the affected company's existing security program.[211] Incorporating a "notice and cure" provision into its statute is a way the Pennsylvania legislature can balance the protection of consumers' biometric data security and also provide businesses an avenue of relief, while ultimately ensuring the continuous enhancement of reasonable security practices.[212]

## V. CONCLUSION

Biometric data technology will become ubiquitous, with its applications increasing across a variety of fields.[213] With these innovative uses of biometrics comes the potential for serious consequences involving cyber hacking and data breaches,[214] sometimes leaving victims of these breaches without proper recourse. It is not only important for individuals, companies, and other entities to keep up with their own reasonable security and compliance measures, but state legislatures must also take on the responsibility of creating biometric data protections for consumers and provide companies with effective guidelines on how to safeguard this sensitive data.

To ensure proper protections of its consumers' biometric data, it is essential for the Pennsylvania legislature to take action and enact state legislation for the protections and benefits of both consumers and companies. The privacy interests of Pennsylvania citizens

207. *See* COOLEY LLP, *supra* note 205.
208. *See* Perez & Rockwell, *supra* note 204.
209. *See generally id.*
210. *Id.*
211. *Id.*
212. *Id.*
213. *See* Craig Oliver, *Technology at a Price: Risks with Using Biometric Scanning in the Workplace*, BRADLEY (Feb. 27, 2019), https://www.bradley.com/insights/publications/2019/02/technology-at-a-price-risks-with-using-biometric-scanning-in-the-workplace.
214. Thakkar, *supra* note 26.

outweigh waiting to enact one uniform federal standard, and it may only be a matter of time before a catastrophic data breach occurs leaving victims without proper protections and recourse. Failing to create legislation protecting rights for consumers' biometric data protection with the Pennsylvania Constitution's strong values of privacy would be ignoring these fundamental principles embedded in the Pennsylvania legal system.[215] Pennsylvania has the potential to construct a statute that may serve as a model of its own to the rest of the nation and inspire trust and uniformity in the realm of biometric data protection. Thus, Pennsylvania must seize this opportunity to protect its citizens' biometric data, and it must do so before this data is compromised.

215. *See* PA. CONST. art. I, § 1, 8.