"HE'S GOT *YOUR* EYES!": ENACTING A FEDERAL BIOMETRIC DATA PRIVACY STATUTE TO SECURE PRIVACY RIGHTS FOLLOWING THE TECHNOLOGICAL SHIFT TO DIGITAL PLATFORMS

By: Emma Myles[*]

I. DEFINING THE CURRENT STATE OF BIOMETRIC DATA PRIVACY RISKS AND PROTECTIONS 256
A. AN OVERVIEW OF THE BIOMETRIC DATA PRIVACY REGULATORY LANDSCAPE. 259
1. Domestic Regulations. 259
2. Federal Biometric Data Privacy Attempts. 261
3. Foreign Regulations. 262
II. THE EVOLUTION OF PRIVACY RIGHTS: CONSIDERATIONS FOR ENACTING A FEDERAL BIOMETRIC DATA PRIVACY STATUTE 265
A. EXPANDING THE CONSTITUTIONAL RIGHT TO PRIVACY TO ADDRESS PUBLIC ENTITY OVERREACH. 265
B. SHIFTING THE ECONOMIC BURDEN OF BIOMETRIC DATA COLLECTION AND PROTECTION. 267
1. The Ubiquity of Biometric Information and its Technological Application. 267
2. Private Entities Must Bear the Burden of Biometric-Identifier Use. 269
3. Disincentivizing Businesses Should not Take Priority in Regulating Biometric Data Privacy. 269
C. PUBLIC POLICY IS BETTER SERVED WHEN INDIVIDUALS ARE IN CONTROL OF THEIR BIOMETRIC INFORMATION. 270
III. DRAFTING CONSIDERATIONS FOR AN EFFECTIVE BIOMETRIC DATA PRIVACY REGULATION 271
A. BIPA SHOULD BE THE FLOOR FOR BIOMETRIC DATA PRIVACY LEGISLATION. 271

[*] University of Houston Law Center, J.D. Candidate 2023, Chief Articles Editor of the Houston Business and Tax Law Journal, Board 23. Thank you to Board 23 for your time and efforts with this article. I would also like to thank the attorneys and staff at O'Hagan Meyer in Chicago for introducing me to this topic and Professor Nikolas Guggenberger for his thoughtful suggestions. Finally, I would especially like to thank my sister, my fiancée, and my family and friends for their tireless encouragement while writing this article and throughout my law school journey.

B. ANALYZING IMPORTANT BIOMETRIC DATA PRIVACY PROVISIONS CONTAINED IN OTHER STATE REGULATIONS. 274
C. ENSURING THE ENACTED BIOMETRIC PRIVACY LEGISLATION ADAPTS WITH CHANGING TECHNOLOGY. 275
IV. CONCLUSION 276

I. DEFINING THE CURRENT STATE OF BIOMETRIC DATA PRIVACY RISKS AND PROTECTIONS

From fingerprints to facial recognition, biometric data is collected through many of the devices individuals use every single day.[1] Biometric information or biometric data encompasses unique biological identifiers such as fingerprints, retina scans, iris scans, palm prints, voice recognition, facial-geometry recognition, DNA recognition, gait recognition, and scent recognition.[2] Despite the existence of some federal data privacy laws,[3] the general use, collection, or sale of an individual's biometric data remains largely unprotected.[4] A few states have enacted biometric-data-specific legislation,[5] but most states currently lack any biometric data protection.[6] Moreover, nearly forty percent of states have no clear plan to propose any legislation protecting biometric data privacy.[7] Consequently, with the increase in digital transactions,[8] cybercrimes,[9] and the frequency with which biometric

1. *Biometric-enabled Active Phones in North America, Western Europe & APAC 2016-2020*, STATISTA RSCH. DEP'T, (Sept. 22, 2021), https://www.statista.com/statistics/1226088/north-america-western-europe-biometric-enabled-phones/; Dan Rafter, *Biometrics and biometric data: What is it and is it Secure?*, NORTON (Oct. 6, 2022), https://us.norton.com/blog/iot/what-is-biometrics.

2. 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.

3. *See* Freedom of Information Act, 5 U.S.C. § 552(a); *see also* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801–6809; Health Insurance Portability and Accountability Act of 1996 (HIPPA), 42 U.S.C. § 1320(d)(6) (providing that biometrics are considered "[i]ndividually [i]dentifiable [h]ealth [i]nformation" and, as such, healthcare workers must ensure proper safeguarding).

4. *See* discussion *infra* Section I.A. Though, HIPPA requires patient biometric information receive a heightened standard of protection, the scope of the statute's applicability is limited to those handling biometric information in the healthcare context. *See* HIPPA § 1172 (defining applicability).

5. *See* Illinois Biometric Information Privacy Act (BIPA), 740ILL. COMP. STAT. 14/1; *see also* Texas Capture of Use of Biometric-Identifiers Act (CUBI),11 TEX. BUS. & COM. § 503.001; N.Y. LAB. LAW § 201-a; WASH. REV. CODE § 19.375.010 (2017).

6. *See* Amy de La Lama & Lauren J. Caisman, *U.S. Biometric Laws & Pending Legislation Tracker*, BRYAN CAVE LEIGHTON PAISNER LLP, https://www.bclplaw.com/en-US/events-insights-news/u-s-biometric-laws-pending-legislation-tracker.html (Feb. 16, 2022).

7. *See id.* (illustrating that 18 states have not proposed any legislation regarding the protection of biometric data).

8. Lindsay Anan et al., *US Digital Payments: Achieving the Next Phase of Consumer Engagement*, MCKINSEY & CO.: PAYMENTS | DIGIT. AND ANALYTICS (Nov. 25, 2020), https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/us-digital-payments-achieving-the-next-phase-of-consumer-engagement.

9. Rob Sobers, *134 Cybersecurity Statistics and Trends for 2021*, VARONIS, https://www.varonis.com/blog/cybersecurity-statistics/ (July 8, 2022).

data is used, collected, and sold,[10] a federal shield is required to protect each citizen's biometric data.

Indeed, the fact that the United States continuously fails to provide federal biometric data privacy protections sets it far behind other developed countries.[11] A 2021 two-part study ranking 96 countries by their respective "collection and use of biometric data" as well as the presence of "restrictions and regulations regarding biometric use and surveillance," or lack thereof, determined that the U.S. initially ranked fourth-worst.[12] This was due to the staggering lack of specific biometric data protection for its citizens coupled with the increased prevalence of biometric identifying technology.[13] As part of the "bottom 5," the U.S. joined Saudi Arabia, Iran, Iraq, and China.[14] For the second part of the study, the U.S. ranking dropped to third-worst when the study also considered each 'country's use of biometric data "to control the spread of COVID-19."[15] While the U.S. increased its' score by a couple points in a 2022 update of the study, it still remained one of the "worst-scoring countries for biometric data collection."[16]

These low scores translate into increased risks for citizens in the U.S., including increased identity theft[17] and the prevalence of deepfakes.[18] Onifido, a global identity verification and authentication provider, published in their 2022 study that there was an increase in

---

10. Justina Alexandra Sava, *Global Biometric System Market Revenue from 2020 to 2027*, STATISTA RSCH. DEP'T. (Oct. 7, 2022), https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/.

11. *See* Paul Bischoff, *Biometric Data: 96 Countries Ranked by How They're Collecting it and What They're Doing with it*, COMPARITECH (Jan. 27, 2021) (on file with the author); *see also* discussion *infra* Sections I.A.2 and I.A.3.

12. Bischoff, *supra* note 11.

13. *See id.*

14. *Id.*

15. *Id.* (citing the decrease in rank to the implementation of Amazon One's palm-scanning payments, fever detection cameras, and facial recognition technology that will work with masks in airports).

16. *See* Paul Bischoff, *Biometric Data: 100 Countries Ranked by how They're Collecting it and What They're Doing with it*, COMPARITECH, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/ (Apr. 4, 2022) (citing a lack of specific protections for U.S. citizens' biometric information despite increased use of "facial recognition in public places, biometrics within the workplace, and fingerprints for visas.").

17. *See New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020*, FED. TRADE COMM'N (Feb. 4, 2021), https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers (reporting that identity fraud incidents increased to around 45% for American citizens). *See also* Sam Cook, *Identity Theft Facts & Statistics: 2019-2022*, COMPARITECH (Oct. 7, 2022), https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/.

18. Generally, deepfakes are media, such as a video or photos, using a real person's image or other biometric information to create a false impression that it is the same person making the statements or engaging in the actions. *See* Chiradeep BasuMallick, *What Is Deepfake? Meaning, Types of Frauds, Examples, and Prevention Best Practices for* 2022, SPICEWORKS (May 23, 2022), https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-deepfake/.

organized fraud activity entering the marketplace where large-scale illicit operations have the resources to use deepfakes.[19] However, at least one company claims that its detection program can identify a deepfake creation with 96% accuracy; that is, if you are willing to pay for the software.[20] Free deepfake-detecting programs appear to be less accurate, with one platform identifying a deepfake image with 69% certainty but then incorrectly identifying another deepfake image as authentic with 54% certainty.[21] Deepfakes entail great political risks, such as: providing false statements to influence politics, enabling the use of manipulated sound clips as evidence, or even the creation of fake pornographic videos.[22]

Beyond the risk of deepfakes, currently, biometric information is captured at the border,[23] handed over to private companies for DNA testing,[24] and used to prevent entry into venue spaces,[25] with little to no protection or regulation. Accordingly, this comment argues for the enactment of a federal biometric data privacy statute to cover citizens in states lacking any protections and to further standardize the asymmetrical protections provided by some states. To present an overview of the more recent regulatory landscape, Section I.A.1. will first examine state legislation targeting biometric data privacy. Then, Section I.A.2. will analyze a few federal attempts at enacting a biometric data privacy statute. Section I.A.3. will highlight different approaches to regulating biometric data privacy at the national level by examining current foreign legislation structures.

Next, Section II.A. of this comment will address the intersection between constitutional protections and biometric data privacy. Section II.B. will discuss biometric data use by private entities as well as the

---

19. *Surge in Sophisticated Fraud Points to Increase in Organized Crime Rings says new Report*, SEC. INFOWATCH.COM (Dec. 8, 2021), https://www.securityinfowatch.com/retail/press-release/21249497/onfido-surge-in-sophisticated-fraud-points-to-increase-in-organized-crime-rings-says-new-report.

20. Billy Perrigo, *How to Spot and AI-Generated Image Like the 'Balenciaga Pope'*, TIME (Mar. 28, 2023, 2:24 PM), https://time.com/6266606/how-to-spot-deepfake-pope/.

21. *Id.*

22. EUR. PARLIAMENTARY RSCH. SERV., PANEL FOR THE FUTURE OF SCI. AND TECH., *Tackling deepfakes in European policy*, at 34-35 (July 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf.

23. *A Federally Mandated Entry-Exit Tracking System Remains Incomplete After a Quarter-Century. Where do we go from here?*, NAT'L IMMIGR. F. (Mar. 22, 2022), https://immigrationforum.org/article/biometrics-at-the-border/#Themes-In-Washington-This-week.

24. Victoria McIntosh, *DNA Testing Kits: What are the Privacy Risks?*, COMPARITECH, https://www.comparitech.com/blog/information-security/dna-testing-kits-privacy-risks/ (June 1, 2022).

25. Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban its Owner's Enemies*, THE N.Y. TIMES, https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html (Jan. 3, 2023).

economic impact of enacting a federal biometric data privacy statute. Importantly, Section II.C. will advance public policy concerns that a comprehensive federal statute may address.

Section III.A. of this comment will recommend that any federal biometric data privacy statute should use the Illinois Biometric Information Privacy Act (BIPA) as the legislative floor, as it remains one of the most stringent biometric-data-privacy-specific statutes in the U.S.[26] Section III.B. will highlight a few worthwhile biometric data privacy provisions found in other existing state statutes. Finally, Section III.C. will address how the statute, faced with the changing nature of technology, may maintain adaptability through rights-focused drafting.

A. AN OVERVIEW OF THE BIOMETRIC DATA PRIVACY REGULATORY LANDSCAPE.

1. Domestic Regulations.

Presently, the oldest and most robust biometric-data-privacy-specific statute in the U.S. was enacted in Illinois in 2008.[27] BIPA provides safeguards on how an entity is supposed to retain, collect, disclose, and destroy biometric data.[28] The statute contains penalties of $1,000 for each negligent violation and $5,000 for each intentional violation.[29] It is also the only biometric data privacy legislation in the country that provides for a private cause of action and awards attorneys' fees.[30] In 2019, the Illinois Supreme Court expressly held that a person does not have to suffer actual or concrete harm to have standing under BIPA—a mere violation is enough.[31] Predictably, this decision has made Illinois rife with class action lawsuits[32] and has even resulted in one of the largest consumer privacy settlements in U.S. history.[33]

---

26. *See* David J. Oberly, *Complying With the World's Most Stringent Biometric Privacy Law*, Ohio State Bar Ass'n (Mar. 24, 2020), https://www.ohiobar.org/member-tools-benefits/practice-resources/practice-library-search/practice-library/2020OL/complying-with-the-worlds-most-stringent-biometric-privacy-law/.

27. 740 ILL. COMP. STAT. 14/5 (2022); *The Evolution of Biometric Data Privacy Laws*, BLOOMBERG L. (Jan. 25, 2023), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/.

28. *Id.* § 14/15.

29. *Id.* § 14/20.

30. Prescott, *supra* note 2; *see also* 740 ILL. COMP. STAT. 14/20.

31. *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019).

32. Richard R. Winter et al., *BIPA Update: Class Actions on the Rise in Illinois Courts*, HOLLAND & KNIGHT (July 22, 2019), https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts.

33. Jennifer Bryant, *Facebook's $650M BIPA Settlement 'a make-or-break moment'*, INT'L ASS'N OF PRIV. PROS. (Mar. 5, 2021), https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/.

By contrast, even though Texas and Washington have biometric-specific data privacy laws, neither state provides for a private cause of action.[34] In Texas, the Capture or Use of Biometric-Identifier Act (CUBI) imposes a civil penalty of $25,000 for each instance where, without prior consent, a biometric identifier is "captured" or sold, as well as for each instance where a biometric identifier is either not stored with reasonable care or not destroyed within a reasonable time.[35] However, only the state attorney general has the exclusive authority to enforce those rights.[36]

Similarly, in the Washington Biometric Privacy Act (WBPA), no company or individual may enter biometric information into "a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[37] Further, like Texas, it also exclusively authorizes enforcement by the attorney general.[38]

Another prominent regulation is the California Consumer Privacy Act of 2018 (CCPA) which provides individuals with a means to control the personal data that businesses collect.[39] The regulation broadly protects consumer privacy by providing a right to know, delete, and opt-out of having personal information collected, used, or sold. Additionally, the statute provides for a right of non-discrimination for an individual's excursion of his or her right.[40] Approved in November 2020, the California Privacy Rights Act of 2020 (CPRA) amended the CCPA to include a new right to correct inaccurate personal information as well as a right to limit the use and disclosure of sensitive personal information, which took effect on January 1, 2023.[41] Further, the CPRA established the California Privacy Protection Agency (CPPA) "to implement and enforce" the CCPA.[42] Though the statute regulates consumer privacy generally, biometric information is included under the types of "personal information" that are subject to protection.[43]

---

34. Prescott, *supra* note 2.

35. TEX. BUS. & COM. CODE ANN. § 503.001.

36. *Id.*

37. WASH. REV. CODE ANN. § 19.375.020 (West 2017).

38. *Id.* § 19.375.030

39. OFF. OF THE ATT'Y GEN., STATE OF CAL. DEP'T OF JUST., *California Consumer Privacy Act (CCPA),* https://oag.ca.gov/privacy/ccpa (Feb. 15, 2023).

40. *Id.*

41. *Id.*; OFF. OF THE ATT'Y GEN., SUBMISSION OF AMENDMENTS TO THE CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT OF 2020, VERSION 3, NO. 19-0021, AND REQUEST TO PREPARE CIRCULATING TITLE AND SUMMARY (AMENDMENT) (NOV. 4, 2019).

42. OFF. OF THE ATT'Y GEN., STATE OF CAL. DEP'T OF JUST., *CCPA Regulations,* https://oag.ca.gov/privacy/ccpa/regs (last visited Apr. 2, 2023).

43. *See* CAL. CIV. CODE § 1798.140(v)(1)(E); *Id.* § 1798.140(c)(defining "biometric information" as "an individual's physiological, biological, or behavioral characteristics, including . . .

Other states that have adopted legislation protecting biometric data include Arkansas, which follows California's CCPA model,[44] and New York, with context-specific protections. Primarily, New York broadened its 2019 Stop Hacks and Improve Electronic Data Security Act (commonly referred to as the SHIELD Act), which focuses on data breaches, to include biometric information.[45] Additionally, the state also passed a narrower biometric data privacy legislation that prohibits fingerprinting "as a condition of securing employment or of continuing employment."[46] Neither law expressly provides for a private right of action.

Notably, all but nine states have at least attempted to introduce biometric data privacy legislation ranging from simply requiring businesses to disclose what information it collects to providing for liquidated statutory damages or actual damages for privacy violations.[47] Conversely, some states are even proposing legislation to repeal existing biometric data privacy laws.[48] These disparities and legislative uncertainties create difficulties for commercial entities, employers, and individuals to engage with each other while fully understanding their respective rights and liabilities.

2. Federal Biometric Data Privacy Attempts.

There have been several federal attempts to enact biometric data privacy legislation. The Commercial Facial Recognition Privacy Act of 2019 was limited in scope in that it only focused on facial recognition technology.[49] The Act barred the collection of facial recognition data unless there was notice and consent.[50] It recognized a singular affirmative defense if the end-user destroys the biometric data upon the discovery that the individual did not give consent.[51] It even applies during a "mass-scanning" of faces in spaces where individuals do not have a reasonable expectation that facial technology is being used on

---

[DNA,] that is used or intended to be used . . . to establish individual identity . . . [including,] imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as faceprint, a minute 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.").

44. ARK. CODE ANN. § 4-110-103(7) (West 2019) (revising the definition of personal information to include biometric data).

45. N.Y. GEN. BUS. LAW § 899-aa(b)(i)(5).

46. N.Y. LAB. LAW § 201-a (McKinney 2014).

47. *Tracking Privacy Legislation by State*, BLOOMBERG L. (July 29, 2021), https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/.

48. *Id.*

49. Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).

50. *Id.*

51. *Id.*

them.[52] Yet, the Act provides a loophole for companies like *Ever* which advertise themselves as cloud-saving applications but use uploaded content to increase the efficacy of their facial recognition algorithms.[53]

The Consumer Online Privacy Rights Act focused on creating rights instead of barring specific conduct.[54] The Act provides for a right to access and transparency, a right to delete, a right to correct inaccuracies, a right to control, a right to data minimization, and a right to data security.[55] Senator Maria Cantwell, the author of the bill, views it as the *Miranda* rights for the digital age.[56] For enforcement of these rights, Cantwell calls for the establishment of a new bureau in the FTC.[57] Most importantly, this bill still allows states to create privacy laws as well as enforce them.[58]

The Online Privacy Act of 2019, proposed by California representatives, does not explicitly protect biometric data.[59] Rather, it protects personal information held or stored by specific corporate entities that is "linked or reasonably linkable to a specific individual."[60] Primarily, the Act ensures the right to access, correct, or delete data.[61] Additionally, the Act provides the right to portability, human review of automated decisions, individual autonomy, notice, consent, and impermanence.[62]

3. Foreign Regulations.

It is also necessary to examine successfully enacted foreign biometric data privacy regulatory schemes. Most emblematic of this international focus is the European Union's (EU) robust General Data Protection Regulation (GDPR), which stands at the forefront of all modern national data privacy regulations.[63] The GDPR requires a legal basis for any entity to process personal data, including biometric data, and it provides that every individual has the right to privacy and data

---

52. *Id*.

53. *See* Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools.*, CNBC, https://www.cnbc.com/2019/05/09/ever-developed-facial-recognition-tools-using-photos-uploaded-to-app.html(May 10, 2019, 5:26 PM).

54. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

55. *Id.* §§ 102–07.

56. Press Release, Maria Cantwell United States Senator For Washington, Cantwell, Senate Democrats Unveil Strong Online Privacy Rights (Nov. 26, 2019), https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights.

57. Consumer Online Privacy Rights Act, S. 847 116th Cong. § 301(a)(1)(2019).

58. *Id*. §§ 301(b), 302(b).

59. *See* Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019).

60. *Id.*

61. *Id.*

62. *Id.*

63. *Tackling deepfakes in European* policy, *supra* note 22.

protection.[64] The GDPR has been adopted in 28 countries in the EU and the United Kingdom.[65] This regulation ensures that individuals have the right to withdraw their consent at any time, entities must notify authorities within 72 hours upon discovering a data breach, and massive penalties will be enforced against companies that fail to adequately secure biometric data.[66]

India continues the global acknowledgment of biometric data privacy concerns by providing protection to its citizens. Once over the age of 18, each Indian resident is assigned a unique 12-digit completely digital identification number, which contains all captured biographic and biometric data related to that person.[67] This data is referred to as Aadhaar data.[68] Over 99% of adults have received a number and the number is then used to "authenticate" an Indian resident.[69] In 2017, their supreme court ruled that privacy was a "fundamental right" and that private companies may not use Aadhaar data.[70] However, in 2019, the passage of new laws allowed private companies to use an individual's Aadhaar data for verification purposes.[71] Crucially, collection is still prohibited.[72]

China introduced its Cybersecurity Law (CSL) in 2017, which includes biometric data in its definition of personal information.[73] The country extended this law in 2018 with the Personal Information Security Specification, which details how personal information should be used and stored.[74] Though China's approach increases consumer privacy protections against private parties, it does nothing to protect citizens against the Republic's power to collect their information.[75] For example, if the Chinese government requests access to personal

---

64. *Id.*

65. *Biometric data and privacy laws (GDPR, CCP/CRPA)*, THALES GROUP, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data (last updated Jun. 16, 2021).

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.*

70. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

71. *Biometric data and privacy laws (GDPR, CCP/CRPA)*, *supra* note 41.

72. *Id.*

73. *Id.*

74. Mingli Shi et al., *Translation: China's Personal Information Security Specification*, NEW AM. (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/; *see* Guo Bing v. Hangzhou Wildlife World (郭兵与杭州野生动物世界有限公司服务合同涉人脸识别纠纷) [Guo Bing v. Hangzhou Wildlife World], (Primary People's Ct. 2020) (China) (ordering a local safari animal park to delete facial information collected without the owner's consent in China's first facial-biometrics litigation).

75. Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 PENN. ST. J.L. & INT'L AFF. 49, 107 (2020).

information from any company, there is no restriction in the CSL that bars this infringement.[76]

Brazil and South Africa have also enacted similar legislative schemes to the EU's GDPR and California's CCPA. In 2018, Brazil passed the Lei Geral de Proteção de Dados Pessoais or General Data Protection Law (LGPD), which protects "the fundamental rights of freedom and privacy and the free development of the personality of the natural person."[77] The LGPD applies to "any natural person or entity, public or private," regardless of whether they exist outside of Brazil.[78] Pointedly, the legislation provides heightened protection for "sensitive" personal information like racial origin or genetic or biometric data.[79] Effective as of July 1, 2021, the Protection of Personal Information Act (POPIA) of South Africa nearly identically regulates the use of biometric information.[80]

Though there are several distinct models for comprehensive biometric data privacy protections, some of these models also overlap in critical privacy rights areas. Primarily, each national scheme restricts the processing of personal information by private or third parties. Furthermore, most seem to contain some form of an informed consumer consent provision, penalties for failing to secure biometric data, and the ability for an individual to control an entity's possession of their biometric information. Finally, while the GDPR, LGDP, and POPIA apply to both public and private entities without exception, current state biometric data privacy legislation conveniently exempts public entities from holding any liability. Why should public entities be exempted from adhering to biometric data privacy protections, especially in the United States?

---

76. *Id.* at 107 n.286.

77. Sarah L. Bruno, *The LGPD: Brazil's data privacy law gains more teeth*, REED SMITH (Sept. 10, 2020), https://www.reedsmith.com/en/perspectives/2020/09/the-lgpd-brazils-data-privacy-law-gains-more-teeth.

78. *Id.*

79. *Id.*

80. *South Africa Personal Information Act*, INT'L TRADE ADMIN. (Sept. 1, 2020), https://www.trade.gov/market-intelligence/south-africa-personal-information-act; Protection of Personal Information Act 4 of 2013 § 58(2) (S. Afr.).

II. THE EVOLUTION OF PRIVACY RIGHTS: CONSIDERATIONS FOR ENACTING A FEDERAL BIOMETRIC DATA PRIVACY STATUTE

A. EXPANDING THE CONSTITUTIONAL RIGHT TO PRIVACY TO ADDRESS PUBLIC ENTITY OVERREACH.

Privacy, as a right, has been a primary concern for justices of the U.S. Supreme Court since 1890.[81] Over a century ahead of their time, Justices Brandeis and Warren co-authored an article on the right to privacy in which they argued that the definition must be expanded to fully protect all aspects of "a right to enjoy life."[82] With incredible foresight, the two Justices even articulated that this right to privacy should extend to "facial expression[s]."[83] This perspective, that the definition of the right of privacy should encompass more than tangible or intangible property rights, is further argued by Justice Brandeis in the dissent of *Olmstead v. United States*.[84] In *Olmstead*, the Court affirmed that there was no violation of the defendants' Fourth Amendment rights when the government proffered wire-tapping evidence to secure a conviction, as the Amendment only applied to physical searches and seizures.[85] Justice Brandeis took issue with the majority's textualist view and pointed out that to truly ensure an individual's protection against government abuses of power, the Constitution must adapt.[86]

Thankfully, in *Katz v. United States*, the Court discounted the traditional interpretation of the Fourth Amendment by holding that a violation can occur even without a physical intrusion.[87] Further, in *United States v. Jones*, the majority found that installing a GPS device on the defendant's car constituted a "search" under the Fourth Amendment's protection for "effects."[88] While Justice Sotomayor agreed with the holding of the case, she also indicated a privacy concern with how much information a GPS captures.[89] Specifically, Sotomayor

---

81. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("The right to life has come to mean the right to enjoy life, —the right to be let alone . . . .").

82. *Id.*; *see* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383 (1960); *see also* Joshua J. Kaufman, *The Invention that Resulted in the Rights of Privacy and Publicity*, VENABLE LLP (Sept. 24, 2014), https://www.venable.com/insights/publications/2014/09/the-invention-that-resulted-in-the-rights-of-priva ("What threat motivated these gentlemen to feel a need to articulate this new doctrine and protection? It was the development of a nefarious, threatening and dangerous device, the *hand-held camera*.").

83. Warren & Brandeis, *supra* note 81, at 206.

84. *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

85. *Id.* at 466.

86. *Id.* at 473.

87. *Katz v. United States*, 389 U.S. 347, 351 (1967).

88. *United States v. Jones*, 565 U.S. 400, 404 (2012).

89. *Id.* at 415-16 (Sotomayor, J., concurring). Nearly four decades before *Jones*, the majority acknowledged Justice Sotomayor's concern about the dangers to privacy that are implicated with the aggregation of personal data in *Whalen v. Roe*, 429 U.S. 589, 605 (1997) ("We are not unaware

suggests that GPS information can create a profile of the individual, which can increase the potential for abuse by law enforcement agencies.[90]

More recently, the Court has adopted differing opinions on what it considers to be a search and seizure violation under the Fourth Amendment based on whether the surveillance occurs in a public or a private space.[91] In C*arpenter*, the majority held that even though a collection of an individual's cell-site location information (CSLI) was similar to a GPS, the important distinction is that the CSLI also captures past movements.[92] Therefore, the collection of this information constituted a search under the Fourth Amendment and is not negated by the fact that this information is held by a third party in this instance.[93]

It is important to note the Supreme Court has contemplated that other Amendments in the Constitution may also defend against invasions of privacy by the government.[94] In *Stanley v. Georgia*, Justice Marshall stated that the First and Fourteenth Amendments fundamentally include a "right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy."[95] Justice Douglas, in *Griswold v. Connecticut*, articulated that the specific guarantees in the Bill of Rights created "penumbras" to "help give them life and substance," such as a right of privacy.[96]

Utilizing the above cases, we begin to examine what privacy rights are likely to be protected by the Court against public entities under the Constitution and the gaps a comprehensive federal regulation could fill. Increasingly, Justice Sotomayor's concern in *Jones* is becoming a reality with the rapid integration of portable information collectors through the interconnectivity of various technology devices, commonly referred to as the Internet of Things (IoT),[97] and its potential to create

---

of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.").

90. *Id.* at 416.

91. *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

92. *Id.* at 2216.

93. *Id.* at 2217.

94. U.S. CONST. amend. I. (providing freedom to choose any kind of religious belief and to keep that choice private); U.S. CONST. amend. III. (protecting the zones of privacy in the home); U.S. CONST. amend. V. (providing for the right against self-incrimination, which justifies the protection of private information); U.S. CONST. amend. IX. (previously interpreted to justify a broad reading of the Bill of Rights to protect a fundamental right to privacy).

95. *Stanley v. Georgia*, 394 U.S. 557, 564 (1969).

96. *Griswold v. Connecticut*, 381 U.S. 479, 484–85 (1965).

97. FTC, *Internet of Things: Privacy & Security in a Connected World 6* (2015) [hereinafter Internet of Things], http://bit.ly/2Eexg2f (defining the IoT as "'things' such as devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information with or between each other through the Internet.").

increasingly accurate information profiles of individual people.[98] Are public entities subject to any restrictions in using this information? What protections are afforded to citizens under the Constitution?

B. SHIFTING THE ECONOMIC BURDEN OF BIOMETRIC DATA COLLECTION AND PROTECTION.

1. The Ubiquity of Biometric Information and its Technological Application.

With the increased development of technology, biometrics are widely utilized to accurately and effectively identify individual human faces.[99] In 2019, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) tested the efficacy of a facial recognition algorithm using databases containing 12 million people which resulted in an error rate of below 0.2%.[100] Five years prior, in 2014, similarly tested algorithms produced error rates between 4.1% to 66.9%.[101] These algorithms are now being deployed across industries and have even gained popularity with celebrities.[102]

On a larger scale, though, employers and commercial entities leverage these algorithms to collect and identify employee or consumer biometric information to cut costs and increase revenue.[103] One popularized example of their usefulness in mitigating labor costs is through fingerprint scanning in lieu of timecards to prevent "buddy-punching."[104] This action occurs when one worker "punches" in for a different hourly worker who is absent.[105] This practice is estimated to

---

98. *See* Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. (forthcoming 2023)(manuscript at 32–35) (noting that period and fertility tracking apps, like many apps, share or sell data as part of a "large data ecosystem" which then may end up in the hands of "law enforcement and intelligence agencies."). Additionally, the authors point out that private actors may be enticed to "leverage consumer data" for "[s]ubstantial bounties proffered by states to restrict abortion access. *Id.* at 38–39.

99. Patrick Grother et al., U.S. DEP'T OF COM., NAT'L INST. OF STANDARDS & TECH., *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification 2* (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

100. *Id.*

101. Patrick Grother & Mei Ngan, *Face Recognition Vendor Test* 3 (2014), https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf.

102. Stefan Etienne, *Taylor Swift Tracked Stalkers with Facial Recognition Tech at Her Concert*, THE VERGE (Dec. 12, 2018, 2:04 PM), https://www.theverge.com/2018/12/12/18137984/taylor-swift- facial-recognition-tech-concert-attendees-stalkers.

103. *See What is Buddy Punching and How to Prevent It*, INTUIT QUICKBOOKS, https://quickbooks.intuit.com/time-tracking/resources/prevent-buddy-punching/ (last visited Feb. 19, 2023).

104. *Id.*

105. *Id.*

cost U.S. employers $373 million each year.[106] Yet, employers are also increasing security with biometrics by controlling access to certain information and securing devices or areas.[107]

Revenue generation is another means for companies to exploit biometric data. One example of this exploitation is when companies, like Facebook, increasingly erode their user privacy settings to allow for the disclosure of more user data.[108] This mass collection of data is then used to craft targeted marketing campaigns that increase Facebook's advertisement revenue.[109]

Interestingly, eye-tracking technology, though often used to analyze supermarket layouts, product labels, and store displays[110], is now being collected via VR headsets.[111] This biometric data is being viewed in conjunction with existing eye-tracking studies to involuntarily gather additional information about users.[112] Ian Taylor Logan provides one frightening scenario: "a marketing company could theoretically purchase data from a VR video game producer, compare the eye-tracking data to behavioral studies about teen impulse control, and use that information to sell clothing to that video game's target demographic."[113] This example begs the question that if private entities want to use a consumer's biometric data, shouldn't they be paying the consumer?

---

106. *Id.*

107. *See* Annemaria Duran, *Understanding the Illinois Biometric Information Privacy Act & Its Relation to Employers,* WORKFORCEHUB (Dec. 27, 2017), https://www.workforcehub.com/blog/understanding-illinois-biometric-information-privacy-act-relation-employers/.

108. *See* Lisa P. Angeles, *Untag Me: Why Federal Judges are Broadly Construing Illinois's Biometric Privacy Law*, 42 CARDOZO L. REV. 349, 382 (2020).

109. *Id.*; *See also What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Priv. Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 8-9 (2012) (prepared statement of Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission, Washington, D.C.) ("Companies can also determine demographic characteristics of a face such as age and gender to deliver targeted ads in real time in retail spaces.").

110. *See Academic marketing and consumer research*, TOBII (2017), https://www.tobii.com/solutions/scientific-research/academic-marketing-and-consumer-research (last visited Feb. 19, 2023) (discussing different marketing studies in which eye tracking has been utilized).

111. Ian Taylor Logan, *For Sale: Window To The Soul Eye Tracking As The Federal Impetus For Federal Biometric Data Protection*, 123 PENN ST. L. REV. 779, 788 (2019).

112. *Id*.

113. *Id*.; *see* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 93 (2014) ("[E]ach type of consumer sensor (e.g., personal health monitor, automobile black box, or smart grid meter) can be used for many purposes beyond that particular sensor's original use or context, particularly in combination with data from other [IoT] devices.").

2. Private Entities Must Bear the Burden of Biometric-Identifier Use.

It is well-established that this area of commerce is particularly unregulated,[114] but who is in a better position to respond to these regulations? The answer is simple: those who collect, use, store, and sell biometric data. By employing the least-cost-avoider theory, which asks which party is better suited to the liability of addressing the issue while incurring the least cost, the entities who use the biometric information should "fix" the problem.[115]

There is a clear knowledge disparity between end-users of platforms like Facebook or Google and the platform itself. A commercial entity would have a far greater understanding of the privacy risks while also being able to protect against those risks. Thus, imposing a greater liability would serve two ends: 1) preventing a potential race to the bottom, where companies erode their user privacy settings to generate more revenue, and 2) acknowledging that these entities are simply better suited for the task.

3. Disincentivizing Businesses Should not Take Priority in Regulating Biometric Data Privacy.

Balancing business considerations against consumer protections in drafting biometric data privacy regulations sets up a false equivalency. Some may argue that strict biometric data privacy regulations have affected and will continue to affect technological development and enhanced security efforts.[116] To begin, these arguments fail to acknowledge and appreciate the extremely sensitive nature of biometric information. If an employer's database is breached in pursuit of biometric information, can the individual be made whole after the breach? Fingerprints that employers collect during clock-ins to reflect accurate payroll information are also attached to individuals who must go their entire lives with the same set of fingerprints. Thus, taking a strict approach to regulating biometric information at the outset encourages entities to be proactive in obtaining consent, securing the collected biometric data, and destroying collected biometric data upon completion of its usage.

---

114. *See supra* Section I.

115. Paul Rosenzweig, *Cybersecurity and the Least Cost Avoider*, LAWFARE (Nov. 5, 2013, 11:41 AM), https://www.lawfareblog.com/cybersecurity-and-least-cost-avoider.

116. *See* 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, 352 (2019).

C. PUBLIC POLICY IS BETTER SERVED WHEN INDIVIDUALS ARE IN CONTROL OF THEIR BIOMETRIC INFORMATION.

Keeping up with the demands of modern society necessitates the use of, or interaction with, devices or services that inevitably collect biometric information.[117] Presently, devices like smartphones or tablets—which are equipped to capture a consumer's biometric information—are already in the hands and households of most Americans.[118] This, coupled with an increased desire for the development of biometric systems or technology that incorporates biometrics,[119] fosters an environment where entities are willing to be more invasive for profit while individuals are left with no adequate alternatives.

"No federal statute provides consumers the right to learn what information is held about them and who holds it for marketing or look up purposes."[120] Further, no law requires companies selling consumer data "to allow individuals to review personal information (intended for marketing purposes), control its use, or correct it."[121] This collection, storage, and sale of consumer data is left to the commercial entities and data brokers who profit from the unregulated biometric data privacy landscape.

Public entities should not be immune to these biometric data restrictions. It is a mistaken belief that public entities are better suited to collecting or protecting biometric information.[122] It seems even more

---

117. *See* Rebecca Kelly Slaughter, Remarks of Commissioner for the Open Technology Institute, *Raising the Standard: Bringing Security and Transparency to the Internet of Things?* (July 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter__raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf.

118. *Mobile Fact Sheet*, PEW RSCH. CENTER (April 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile (finding that 85% of Americans own a smartphone device and roughly 50% of Americans own a tablet computer).

119. *Biometrics Technology Market Size Worth $59.31 Billion by 2025: Grand View Research, Inc.*, PR NEWSWIRE (Apr. 18, 2019, 06:35 ET), https://www.prnewswire.com/news-releases/biometrics- technology-market-size-worth-59-31-billion-by-2025-grand-view-research-inc-300834463.html.

120. *What Information Do Data Brokers Have On Consumers and How Do They Use It?: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 113th Cong. 60 (2013) (statement of Alicia Puente Cackley, Dir. of Fin. Mkts. & Cmty. Inv., U.S. Gov't Accountability Office).

121. *Id.*

122. *See* Associated Press in Wash., *US Government Hack Stole Fingerprints of 5.6 million Federal Employees*, THE GUARDIAN (Sept. 23, 2015), https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints; *see also* Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW Rsch. CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (noting that 79% of Americans report being concerned about the way their data is used by companies versus only 64% as concerned with the government doing the same).

imperative that individuals should be able to hold public entities accountable for unauthorized biometric information collection or misuse. Additionally, though public entities may have a legitimate security interest in protecting their constituents, allowing public entities access to this body of information without restriction is a dangerous path to travel down.

For example, prisons are partnering with private companies to engage in the surveillance of incarcerated individuals by collecting biometric data in the form of voiceprints.[123] "As of February 2019, facilities in twelve states are either using or have signed contracts to use Securus Technologies' voice recognition software."[124] Here, the privacy concerns are numerous. Primarily, it is unclear what level of access the private entity that provides the surveillance technology has to the information. Also, the technology can be used, without consent, against individuals who may never be convicted of a crime such as those who are simply awaiting trial or pretrial detainees.[125] Finally, this technology could be employed against those whom inmates contact using prison telephones.[126] Even this singular example highlights the serious privacy concerns with a public entity's unchecked ability to collect, use, and store biometric information.

III. DRAFTING CONSIDERATIONS FOR AN EFFECTIVE BIOMETRIC DATA PRIVACY REGULATION

A. BIPA SHOULD BE THE FLOOR FOR BIOMETRIC DATA PRIVACY LEGISLATION.

Failure to understand the scope of critical language while drafting legislation can leave individuals exposed, with little legal recourse. Thus, BIPA stands out amongst other state biometric data privacy regulations for its forward-thinking privacy protection purpose and explicit provisions.[127] However, due to its enactment in 2008—before much of the current technology at issue came into existence—BIPA lacks some considerations that would make it a more effective and long-lasting biometric data privacy regulation.

---

123. *See* Brock C. Wolf, *An Inmate's Right To Biometric Data Privacy: How Technological Advances Affect Vulnerable Populations*, 11 WAKE FOREST J.L. & POL'Y: SUA SPONTE 81, 83 (2021).

124. *Id.*

125. *Id.* at 94; *Bell v. Wolfish*, 441 U.S. 520, 535–37 (1979) (explaining that loss of privacy is not a punishment, but an "inherent incident[] of confinement in such a facility.").

126. Wolf, *supra* note 123, at 95 (explaining that Securus Technologies has given jail systems the option of covertly extracting voice prints, which allow facilities to collect them from anyone using their phones, and without consent).

127. *See* 740 ILL. COMP. STAT. 14/5 (2008); *see also infra* Section I.A.1.

For example, while BIPA necessarily defines the term "biometric identifier," it includes several limiting exclusions, including "photographs,"[128] which, without some creative judicial intervention, nearly rendered moot several important early BIPA cases.[129] Another significant flaw in this legislation is its vagueness in defining a specific timeline for biometric data retention and destruction. Currently, the statute provides that a private entity must permanently destroy the data collected and retained "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."[130] In short, under BIPA, this leaves a great deal of wiggle room for entities to retain an individual's biometric data for several years. Contrasted with Texas' CUBI which requires that the "person" destroys the biometric identifier "within a reasonable time" but no later than a year after the purpose for collecting the identifier expires, the difference is stark.[131]

Still, despite its legislative blind spots, BIPA is the only statute that provides a private cause of action for aggrieved individuals.[132] The importance of the private cause of action provision cannot be understated. Few statutes allow a private individual to sue an entity in the event of a data breach, and even fewer allow suits based on the improper collection of the data in the first place.[133] Coupled with the Article III standing requirement that a victim must suffer "actual" harm, which can be difficult to establish,[134] BIPA has been a revolutionary statute for protecting individual privacy rights. In the few states with a biometric data privacy statute, individuals may only approach the state

---

128. 740 ILL. COMP. STAT. 14/10 (2008) ("'Biometric 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.").

129. *Norberg v. Shutterfly*, 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015)(denying defendant's motion to dismiss because, even by way of a photograph, defendant was in possession of plaintiff's facial geometry data); *Rivera v. Google*, 238 F. Supp. 3d 1088, 1095-96 (N.D. Ill. 2017)(holding that BIPA's legislative purpose would be frustrated if the legislature meant to limit how biometric identifiers are measured); *In re Facebook Biometric Information Privacy Litigation*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016)(reasoning that "photograph" only applied to physical photographs and not "digitized images stored as a computer file and uploaded to the [i]nternet.").

130. 740 ILL. COMP. STAT. 14/15(a) (2008).

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

132. 740 ILL. COMP. STAT. 14/20 (2008); Myriah V. Jaworkski & Mason N. Floyd, *First of Its Kind BIPA Trial Ends in Blockbuster Judgment*, CLARK HILL (Oct. 19, 2022), https://www.clarkhill.com/news-events/news/first-of-its-kind-bipa-trial-ends-in-blockbuster-judgment/.

133. Michael A. Rivera, *Face Off: An Examination Of State Biometric Privacy Statutes & Data Harm Remedies*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 571, 582 (2019).

134. For example, in the case of a data breach, the "actual" harm may not arise until after the statute of limitations expires. Even under BIPA, establishing harm to satisfy Article III standing was made difficult until *Rosenbach*. *See Rosenbach v. Six Flags Ent't. Corp.*, *supra* note 31.

attorney general to enforce their rights.[135] This approach may come with major uncertainties for individuals looking for a clear remedy. Though state attorneys generally have shaped and protected consumer privacy rights,[136] they still have ultimate discretion regarding which suits they file. Additionally, state attorneys general are elected officials at risk of being solicited by special interest groups to protect their commercial interests.

BIPA is also a legislative trailblazer in distinguishing between the sale and disclosure of biometric data.[137] BIPA does not allow a private entity in possession of biometric data to sell, lease, trade, or otherwise profit from any individual's biometric data.[138] A private entity may disclose, redisclose, or otherwise disseminate an individual's biometric information only if: (1) the individual provides consent; or (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric information; or (3) the disclosure or redisclosure is required by the law or a valid warrant or subpoena.[139] BIPA's separate provisions for the sale of biometric data and disclosure provide extra protection against loopholes through its specificity and wider applicability. Here, having separate provisions to address the sale and disclosure of biometric data matters because in cases where state statutes have addressed each issue in a single provision, it allows for scenarios where the sale of biometric data is allowed.[140]

BIPA addresses, in great detail, the standard that entities are required to employ to protect biometric data.[141] The statute utilizes a two-pronged method composed of both an objective component and a subjective component.[142] First, an entity must use reasonable care in protecting biometric data as defined by the entity's industry.[143] Second, the entity must treat biometric information comparable to how the entity treats its other confidential data.[144]

---

135. *See supra* Section I.A.1.

136. *See* Michael A. Rivera, *supra* note 133 at 586. In the 1960s and 1970s state attorneys general established consumer protection divisions and in the 1990s utilized Unfair and Deceptive Practices statutes to "protect consumers from privacy-invasive business practices."

137. 740 ILL. COMP. STAT. 14/15 (2008).

138. *Id.* at § 14/15(c).

139. *Id.* at § 14/15(d).

140. TEX. BUS. & COM. CODE § 503.001(c) (providing an exemption for identification purposes in the event of disappearance or death); WASH. REV. CODE § 19.375.020 (2017) (providing an exemption for disclosure and sale to any third party who contractually promises to maintain the confidentiality of the data and to not use it for a purpose outside the scope of its original business use).

141. 740 ILL. COMP. STAT. 14/15(e) (2008).

142. *Id.*

143. 740 ILL. COMP. STAT. 14/15(e)(1) (2008).

144. *Id.* § 15(e)(2).

Finally, the Illinois legislature went into painstaking detail in developing the legislative purpose for BIPA. As noted above, the statute was enacted in 2008, when the usage and application of biometric data were likely in their infancy. The legislature noted that major national corporations had begun to use Chicago, as well as other locations in the state, as "testing sites" for new biometric identifier-interpreting technologies.[145] The section emphasizes the individual privacy concerns in employing the use of biometric information and the overall public weariness of biometrics.[146] Most importantly, the section concludes by addressing the importance of regulating biometric technology and all aspects of its collection, retention, and destruction.[147]

B. ANALYZING IMPORTANT BIOMETRIC DATA PRIVACY PROVISIONS CONTAINED IN OTHER STATE REGULATIONS.

Though BIPA is the strictest biometric data privacy statute that exists in the U.S., there are additional points to consider in creating a robust federal regulation. For instance, the WBPA addresses the enrollment rather than the collection of biometric data as compared to BIPA.[148] Under the WBPA, enrollment means "to capture a biometric data identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual."[149] The entity-benefit to this system is derived from what the statute regulates. By focusing on enrollment over the collection, the statute, in effect, only regulates the biometric information that is actually stored in a database to be used for a future purpose.[150] There is also a notable benefit to the consumer through this method. When entities collect biometric identifiers for use, they are required to initially convert the data into a "reference template that cannot be reconstructed into the original" image. This process makes an individual's biometric information more difficult to steal.[151]

Any regulation modeled from BIPA should also take note of Texas' CUBI provision addressing biometric information collection during an employer-employee relationship.[152] This provision states that the purpose for collecting any biometric identifiers expires when the

145. *Id.* § 14/5(b).

146. *Id.* § 14/5(c-d) ("Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.").

147. *Id.* § 14/5(g).

148. WASH. REV. CODE § 19.375.020 (2017).

149. WASH. REV. CODE § 19.375.010(5) (2017).

150. Rivera, *supra* note 133, at 606.

151. *See* § 19.375.020.

152. *See* TEX. BUS. & COM. CODE § 503.001(c)–(c-2) (2009).

employee-employer relationship comes to an end.[153] In sum, employers in Texas must delete any biometric information collected for security purposes when the employee no longer works there.[154] While this seems like a fairly basic and straightforward provision, it considers an entity's purpose for having access to an individual's information. When forming rules and regulations for a constantly evolving subject matter, skilled drafters identify stable elements of an issue to draft around.

C. ENSURING THE ENACTED BIOMETRIC PRIVACY LEGISLATION ADAPTS WITH CHANGING TECHNOLOGY.

The enacted legislation must ensure that entities utilizing biometric identifiers also allow individuals to opt out of providing their biometric information. Biometric authentication can be a way to accurately confirm identification, but from an individual's perspective, there are significant risks to participation, particularly for marginalized populations.[155] Interestingly, cybersecurity experts are not certain that biometric authentication is, in fact, more secure than traditional methods.[156] Providing a meaningful alternative will illustrate the importance of individual privacy rights from an entity perspective. Moreover, an opt-out provision will force entities to first ask for consent to identify how a consumer will elect to interact with them.

The subject matter of this legislation provides a challenge to future drafters because of how abruptly technology can shift. One way to address this issue is through an appointment of special masters. Under Federal Rule of Evidence 706, a court may appoint an expert witness to assist the court in properly understanding the scope of an issue.[157] If the drafters were to adopt BIPA with minimal changes, a neutral, third-party expert could help determine what constitutes "reasonable care" regarding biometric data security best practices.

Finally, considering the nature of technology, drafters should begin with what rights the legislation should protect. The language should be broad when writing about an individual's right to privacy but very specific and intentional when assigning liabilities to entitles. Biometric data is irreplaceable, and the drafters should take into consideration that the current understanding of how information is collected could easily change within the next decade.

---

153. TEX. BUS. & COM. CODE § 503.001(c-2) (2009).

154. TEX. BUS. & COM. CODE § 503.001(c)(3)-(c-2) (2009).

155. *See* Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L. J. F. 907, 917–28 (2022), https://www.yalelawjournal.org/pdf/F7.AllenFinalDraftWEB_6f26iyu6.pdf. Biometric information is at the core of what enables discrimination.

156. Rivera, *supra* note 133, at 574.

157. FED. R. EVID. 706.

IV. CONCLUSION

Ultimately, the argument for a federal statute protecting biometric data privacy is rooted in privacy protections for the individual. Entities interested in collecting, using, or retaining biometric data will adapt to the regulations that assign their liability. Indisputably, public entities as well as many commercial entities were able to accomplish their functions without the use of biometric information in the past. Although technological capabilities in biometric data tracking continue to progress, it should not inherently mean that rights to privacy should be diluted. Entities that cannot function without biometric data regulation should not be allowed to function.

With the increased prevalence of biometric data-identifying technology, it is well-past time for the federal government to enact biometric data privacy legislation in favor of individual privacy. Entities should not have access to immutable information without consent, proper standards for protecting such information, and adequate recourse to the individual for any misuse. As correct then as it is now, Justices Brandeis and Warren expressed that "the protection of society must come mainly through a recognition of the rights of the individual."[158]

158. Warren and Brandeis, *supra* note 81, at 219-20.