Patchwork: Addressing Inconsistencies in Biometric Privacy Regulation

Elisa Cardano Perez*

TABLE OF CONTENTS

* J.D., January 2022, The George Washington University Law School; B.A., International Relations, Northeastern University. Thank you to my colleagues in the Federal Communications Law Journal for their support and diligence in the publication process. A special thanks to Ethan Lucarelli, Journal Adjunct, and Olivia Creser, Notes Editor, for their encouragement and guidance. Finally, I would like to thank my family for their unconditional support.

I. INTRODUCTION

Imagine you are walking into a supermarket. As you walk around the aisles trying to find your favorite chocolate bar, you are unaware that the store's video camera is tracking you. The camera's facial recognition software is used to verify whether you match a criminal database. You exit the store and smoke a cigarette, throwing it into the trash. The cigarette bounces off the rim and hits the ground. A few weeks later, the city square has plastered your face on the billboards of an ad campaign. The cigarette you left on that sidewalk contained some of your DNA and was used to reconstruct your face. This type of campaign was recently employed in Hong Kong to bring awareness to the city's littering problem and shame those who litter.[1] Your DNA was matched with data from the web of commercial firms that collect, share, and sell information. Here, your DNA was matched with the footage from the supermarket that collected your facial template. The matching process facilitated the full reconstruction of your face by the advertisers. These billboards are located all over the city and are equipped with sensors that simultaneously assess the billboards' viewers. These sensors are capable of tracking how long each viewer spends looking at the advertisements, as well as the emotional response of the viewer, by tracking cardiac rhythms and brain waves.

Your phone's notification reminds you about the date that you have planned. A new dating application[2] which matches users based on their DNA compatibility found your perfect match and you must impress that perfect match. Unfortunately, the fingerprint reader of your phone is broken, disabling you from paying at the restaurant through your banking application. You approach an outdated ATM for cash, insert your card into the ATM slot, and verify your identity through facial recognition cameras as a security measure instead of a PIN. The balance has surprisingly decreased. The facial recognition ATM took notice of the campaign, automatically charging you a $200 fine for littering. Anonymity is a luxury in this seemingly dystopian society.

The scenario portrayed above may seem improbable and unimaginable, but it isn't far off from the data privacy concerns of keeping up with the rapid pace of technology governing our newly digitized world. Information, just like time, is money, especially in a world where companies collect and trade on our data points. Biological information gives consumers the ability to secure their information in a way they perceive to be the safest. After all, who could replicate your face or fingertips? The reality of biometric security is that once it is hacked, the information becomes irreplaceable. You can change your credit card number the way you can change your hair color but changing your fingerprint or facial composition—while not impossible—may come at

1. *See* Justin Worland, *Hong Kong Anti-Littering Campaign Uses DNA From Trash to Shame People*, TIME (May 20, 2015, 11:02 AM), https://time.com/3890499/hong-kong-littering-campaign/ [https://perma.cc/WW4C-AGS2].

2. *See* Megan Molteni, *With This DNA Dating App, You Swab, Then Swipe For Love*, WIRED (Feb. 28, 2018, 7:00 AM), https://www.wired.com/story/with-this-dna-dating-app-you-swab-then-swipe-for-love/ [https://perma.cc/LR74-PCRM].

a heftier price. For example, Mr. Kumaran from Malaysia, who secured his car through a fingerprint recognition system, had his index finger cut off by robbers to steal his car.[3] Individuals today have become numb to the habit of using information for "security," and most individuals are not aware of how much information is collected or stored by private firms. Businesses are using biometric information in ways never seen before. These uses range from the use of infrared facial scanners to map out your face for temperature checks, to using facial recognition for confirming restaurant orders or to ensure you are not a criminal.[4]

To maintain some legitimacy and control over our information, more stringent regulation is needed to provide the public with more control over the unwarranted collection, use, and aggregation of biometric information, ensuring that stronger guidelines are in place for companies to follow. The current patchwork of legislation in the United States regarding the collection and use of biometric data is inadequate for both consumers and corporations due to the inconsistencies in the definition of biometric identifiers, the thresholds for consent to collect and use data, the enforcement mechanisms, and the limited access to erase collected data for the public. This Note introduces the problems underlying several of the current legislative regimes governing biometric data in the United States, using them as an analytical framework for a lessons-learned approach for future legislation. Congress should pass a law that enables companies and citizens alike to have consistent protection and consistently applied laws, emphasizing the principle of individual control over information and delineating boundaries for companies to operate within.

Part II, Section A explains the way that biometric technology operates and is used as an identity authenticator. It provides a foundational understanding of the various uses of biometric technology in both the public and private sectors, and explains what individuals lose when they release their private biometric information. Section B describes the different "patches" of legislation in the state and federal systems in the United States, and it introduces the European Union's General Data Privacy Regulation (GDPR), one of the most comprehensive data protection regimes to date. Part II, Section A analyzes the inadequacies of the current statutory framework. It centers the discussion on four main elements: definition of biometric identifiers, consent for collection and use, the right to private action, and the right to data erasure. Section B proposes a federal framework for legislation using a lessons-learned approach, suggesting that the legislation provide for

3. See Jonathan Kent, *Malaysia Car Thieves Steal Finger*, BBC NEWS (Mar. 31, 2005, 10:37 AM), http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm [https://perma.cc/K36M-JUN8].

4. *See* Kristine Argentine & Paul Yovanic, Seyfarth Shaw LLP, *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*, JDSUPRA (June 9, 2020), https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/ [https://perma.cc/U6KP-WCF3]; Jenna Bitar & Jay Stanley, *Are Stores You Shop At Secretly Using Face Recognition on You?*, AM. CIV. LIBERTIES UNION (Mar. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face [https://perma.cc/ZPP5-AFMU].

greater control for individuals and include a more consistent regulatory scheme for firms who operate in this field.

II. BACKGROUND

A. Understanding Biometrics

1. What Are Biometrics and Biometric Systems?

Biometrics refers to the field of methods employed to identify or recognize individuals based on their biological characteristics.[5] These biological characteristics are unique to each human being because they are often innate and immutable.[6] They can be measured by physiological[7] traits, such as a fingerprint, face, or iris,[8] and by behavioral traits that can be recognized by "the way one walks, speaks, writes, or interacts with a computer,"[9] which could be subject to change throughout one's lifetime. Advances in biometric studies have rendered the use of cardiac rhythm (ECG) and electrical activities from the brain (EEG) as possible methods for identification.[10] These modalities for biometric identification remain understudied, but the development of combining methods as a process for identification[11] only continues to evolve as more technology becomes available and as interest in this market grows.

Biometric data is collected and processed using a biometric system. A biometric system works when a sensor captures a biometric trait, extracts that trait's representative feature, and creates a template of that trait that will be stored in the biometric system.[12] Later on, a similar process unfolds to ensure that an input of a trait converted into a template entered will match the previously system-registered template.[13] The biometric sensor captures the

5. *See* Sharon Roberg-Perez, *The Future Is Now: Biometric Information and Data Privacy*, 31 ANTITRUST 60, 60 (2017).

6. *See id.*

7. *See id.*

8. *See What is Biometrics?*, MICH. STATE UNIV.: BIOMETRICS RSCH. GRP., http://biometrics.cse.msu.edu/info/index.html [https://perma.cc/YPH5-YABC] (last visited Aug. 8, 2021).

9. Roberg-Perez, *supra* note 5, at 60 (*citing* NEW DIRECTIONS IN BEHAVIORAL BIOMETRICS 1-2 (Khalid Saeed et al., eds., 2017)).

10. *See* Ramaswamy Palaniappan et al., *Improving the Feature Stability and Classification Performance of Bimodal Brain and Heart Biometrics*, *in* 425 ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING 175, 177, 184 (2016); Ramaswamy Palaniappan, *Electroencephalogram Signals From Imagined Activities: A Novel Biometric Identifier For A Small Population*, *in* INTERNATIONAL CONFERENCE ON INTELLIGENT DATA ENGINEERING AND AUTOMATED LEARNING (IDEAL) 604, 610 (E. Corchado et al. eds., Springer-Verlag Berlin 2006) https://link.springer.com/chapter/10.1007%2F11875581_73.

11. *See* Ramaswamy Palaniappan et al., *supra* note 10.

12. *See What is Biometrics?*, MICH. STATE UNIV.: BIOMETRICS RSCH. GRP., http://biometrics.cse.msu.edu/info/index.html [https://perma.cc/YPH5-YABC] (last visited Aug. 8, 2021).

13. *See id.* There are two types of biometric systems, identification and verification modes. Identification is for large scale use of data bases, whereas verification uses the template stored in the system to ensure that an individual is who they claim to be.

trait, extracts the representative feature, and compares this new template with the previously created and stored template.[14] These "extractable" characteristics that create templates can be derived from varying sources through different technologies.[15]

Legislation typically defines the term "biometric identifiers" as the extractable biometric characteristics used to create the templates that are used and stored within biometric systems.[16] As mentioned, these extractable features can range from faces and irises to cardiac rhythms as new methods of identification are explored.[17] This definition informs corporations of the boundary for collection, use, sale, and extraction of individual biometric features, and what amount of information individuals can expect to be protected.

2. Placing Biometrics in Context: Uses and Privacy Implications

a. Uses of Biometric Information

The breadth of the biometrics market is exemplified through both public and private sector uses. Governments extensively use biometrics for security purposes in law enforcement and immigration control through fingerprinting,[18] and only continue to expand their use. In the United States, the Pentagon developed a laser technology known as the Jetson, which maps cardiac signatures to identify individuals from a distance.[19] Governmental use is evolving to include digital forms of ID that facilitate the provision of services. In India, the *Aadhar* digital ID system is a digital identification number combined with biometric features, such as iris scans,[20] that can be used to validate a citizen's identity by banking institutions, employers, and the government when providing subsidies to its citizens.[21] Russia recently

14. *Id.*
15. *Id.*
16. *See infra* Part II(C)(1).
17. *See What is Biometrics?*, *supra* note 12; Palaniappan et al., *supra* note 10.
18. *See generally Biometrics: Definition, Use Cases and Latest News*, THALES GROUP https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics [https://perma.cc/D2M4-F583] (last updated June 2, 2021) (last visited Aug. 8, 2021).
19. *See* David Hambling, *The Pentagon Has A Laser That Can Identify People From A Distance—By Their Heartbeat*, MIT TECHNOLOGY REV. (June 27, 2019), https://www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/ [https://perma.cc/R4NT-XZVC]; Zak Doffman, *New Pentagon Laser Identifies High-Risk Individuals By Their Heartbeat*, FORBES (June 27, 2019, 10:05 AM), https://www.forbes.com/sites/zakdoffman/2019/06/27/u-s-military-laser-can-identify-people-by-their-heartbeats-mit-reports/?sh=1dfc61d62dc6 [https://perma.cc/T5T4-F2FL].
20. *See* Pam Dixon, *A Failure to "Do No Harm" -- India's Aadhaar Biometric ID Program and its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.*, 7 HEALTH & TECHNOLOGY 539, 544 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5741784/ [https://perma.cc/3ASU-KL53].
21. *See id.* at 544-47.

approved a similar program, where its Unified Biometric System (UBS) will be used by Russian financial institutions.[22] According to the World Bank's *World Development Report on Digital Dividends from 2016*, Belgium, Estonia, Finland, France, the Republic of Korea, and Singapore are some of the countries beginning to transition from physical ID ecosystems to digital ones to deliver services.[23] Aid organizations also employ biometric systems as a method to verify aid distribution in humanitarian crises and refugee administration.[24] As early as 2002, biometric systems were used for iris scans by the United Nations High Commissioner for Refugees (UNHCR) to aid the repatriation of Afghan refugees located in Pakistan.[25]

Like those governments, the private sector is expanding the use of biometric data to promote security, expand access to services, and enhance customer experiences. Apple uses fingerprint[26] and face recognition technology[27] to provide security to customers on their devices. The feature is being enhanced to incorporate heat-mapping, patent-pending technology,[28] that will create a distinctive thermal signature attached to the individual user when using Face ID.[29] Banks may already be collecting voice prints of their customers to avoid access by impersonators.[30] ATMs can be equipped with

---

22. *See* Chris Burt, *Biometric ATMs And Remote Payment Systems Expanding Around The World*, BIOMETRICUPDATE.COM (Jan. 5, 2021), https://www.biometricupdate.com/202101/biometric-atms-and-remote-payment-systems-expanding-around-the-world [https://perma.cc/WDN6-W9L5].

23. *See* WORLD BANK GROUP, WORLD DEVELOPMENT REPORT 2016: DIGITAL DIVIDENDS 194 (2016) https://www.openknowledge.worldbank.org/handle/10986/23347 [https://perma.cc/E7NL-JPZV].

24. *See* Mark Latonero, *Stop Surveillance Humanitarianism*, N.Y. TIMES (July 11, 2019), https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html [https://perma.cc/29EK-2CL4].

25. *See* Katja Lindskov Jacobsen, *Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees*, 46 SEC. DIALOGUE 144, 149 (2015) http://proxygw.wrlc.org/login?url=https://www.jstor.org/stable/26292335; Songkhun Nillasithanukroh, *Rethinking the Use of Biometric Systems for Refugee Management*, CHI. POL'Y REV. (Feb. 24, 2016) https://chicagopolicyreview.org/2016/02/24/rethinking-the-use-of-biometric-systems-for-refugee-management/ [https://perma.cc/3LTP-GVWZ].

26. *Use Touch ID on iPhone and iPad*, APPLE, https://support.apple.com/en-us/HT201371 [https://perma.cc/569Y-B7HB] (last visited Mar. 27, 2021).

27. *Use Face ID on Your iPhone or iPad Pro*, APPLE, https://support.apple.com/en-us/HT208109 [https://perma.cc/2XKR-P3V8] (last visited Mar. 27, 2021).

28. U.S. Patent No. 10,896,318 (filed Mar. 23, 2018); Abdullah, *Apple Patents the Next-Generation Face ID Technology*, GIZCHINA (Jan. 20, 2021), https://www.gizchina.com/2021/01/20/apple-patents-the-next-generation-face-id-technology/ [https://perma.cc/CT2Y-CQHC].

29. '318 Patent.

30. *See Voice Biometrics: The Voice Print Will Become Online Banking's Greatest Ally*, BBVA (Aug. 21, 2020), https://www.bbva.com/en/voice-biometrics-the-voice-print-will-become-online-bankings-greatest-ally/ [https://perma.cc/DAD2-M44K]; Raphael Satter, *Banks Are Harvesting Your 'Voiceprint' On The Phone To See If You're Lying*, BUS. INSIDER (Oct. 13, 2014), https://www.businessinsider.com/banks-use-voiceprint-on-calls-to-detect-fraud-2014-10 [https://perma.cc/BL69-H39G]; Chantal Tode, *Barclays expands use of voice security for phone banking convenience*, RETAIL DIVE https://www.retaildive.com/ex/mobilecommercedaily/barclays-expands-use-of-voice-security-for-phone-banking-convenience [https://perma.cc/MB6C-Y7ZM] (last visited Aug. 8, 2021).

fingerprinting or iris scanning,[31] which are methods being considered in Argentina and Pakistan.[32] Generally, biometric systems will be adopted for security, as previously mentioned, or because they provide greater and faster services to consumers.[33] To provide a new and enhanced service to users in its networks, Facebook launched its "tag" feature, which mapped and extracted facial templates of individuals' photos so that their friends could later "tag" them in photos.[34]

These convenient uses of biometric technology fail to highlight the rapid growth of the biometrics market and the fact that information sharing and data aggregation can lead to the identification of a consumer and their preferences. The market is "expected to grow from USD 36.6 billion in 2020 to USD 68.6 billion by 2025" according to a research report conducted by Markets and Markets.[35] Biometric technology's use in advertising allows marketers to identify consumers' interest in products and how consumers respond to content by measuring their physical responses.[36] Digital signs and kiosks may be equipped with camera lenses, tracking eye movements and facial expressions to decipher attention span and consumer views,[37] while operating under the guise of providing security—that is, checking for shoplifters.[38] If tracked at a store, biometric technology uses a combination of metrics, known as behavioral biometrics, which corporate firms can implement to learn about your preferences.[39] The practices are not entirely transparent. The American Civil Liberties Union informally polled a list of twenty top retailers in the United States on their use of facial recognition on their customers.[40] Only one of the twenty reported not using it, while the

31. *See* Chris Burt, *Biometric ATMs And Remote Payment Systems Expanding Around The World*, BIOMETRICUPDATE.COM (Jan. 5, 2021), https://www.biometricupdate.com/202101/biometric-atms-and-remote-payment-systems-expanding-around-the-world [https://perma.cc/WDN6-W9L5].

32. *Id.*

33. *Id.*

34. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1267-68 (9th Cir. 2019).

35. *See Biometric System Market with COVID-19 Impact by Authentication Type (Single-Factor: Fingerprint, Iris, Face, Voice; Multi-Factor), Offering (Hardware, Software), Type (Contact-based, Contactless, Hybrid), Vertical, and Region, Global Forecast to 2025*, MKTS. & MKTS. (Nov. 2020), https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html [https://perma.cc/YD97-XN28].

36. *See* Susie Hood, *What Is Biometric Marketing Technology & How Can Marketers Use It?*, HITSEARCH (Oct. 15, 2018), https://www.hitsearchlimited.com/news/what-is-biometrics-technology-and-how-can-marketers-use-it [https://perma.cc/D9TN-DYPJ].

37. *Id.*

38. *See* Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores*, N.Y. MAGAZINE: INTELLIGENCER (Oct. 20, 2018), https://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html [https://perma.cc/2WPT-4F3M].

39. *See How Retailers Are Using Biometrics to Identify Consumers and Shoplifters*, EMARKETER (Oct. 3, 2019), https://www.emarketer.com/content/how-retailers-are-using-biometrics-to-identify-consumers-and-shoplifters [https://perma.cc/2T7N-SKK7].

40. *See* Jenna Bitar & Jay Stanley, *Are Stores You Shop at Secretly Using Face Recognition on You?*, AM. CIV. LIBERTIES UNION (Mar. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face [https://perma.cc/G5JB-447V].

others declined to comment or responded that the information was "proprietary" or "confidential,"[41] bringing to attention how individuals lack control over who collects, uses, and controls their uniquely identifying data and the parameters that companies should operate within when it comes to sensitive information.

In its 2030 Report, Essence Advertising surveyed 50 marketing and advertising experts about the future of the industry[42] and reported that leaders in the industry expect biometrics to continue facilitating a more personalized experience in consumers' interactions with products.[43] This means that firms will only continue to enhance their use and collection of biometric information to attract and understand consumer preferences. As noted by Elizabeth Walker in the Fordham Intellectual Property, Media, and Entertainment Law Journal, the private sector may start valuing "fingerprints, eyes, voices, and faces more significantly than the individuals do."[44] If this is the case, individuals' autonomy over control of their data and their ability to share it with companies is essential as this market and the overall field of biometrics continue to evolve.

b. Defining Privacy and Its Implications in the Biometric Sphere

As this field continues its rapid growth, individuals must ask themselves what they will forfeit to use services equipped with biometrics. Alternatively, some may not even be aware their data is being collected without their consent. J.D. Woodward, a scholar on biometrics, presents the debate on privacy in this space as (1) a loss to your individual characteristics uniquely capable of identifying you, and (2) invasiveness of the information to daily life.[45] When an individual discloses a biometric identifier, they are disclosing "accurate" information about their identity.[46] Essentially, an individual forfeits a part of themselves as a data point. Second, there is the possibility that this captured biometric identifier will be easily shared and disclosed to third parties, resulting in loss of anonymity[47] and, as previously mentioned, could be used in conjunction with marketing services to target consumers.[48] When this type of information is gathered and aggregated, it creates a digital identity of an individual existing in an ether of data points,

41. *Id.*

42. *See* Kate Scott-Dawkins & Mark Syal, *Advertising in 2030: Expert Predictions in the Future of Advertising*, ESSENCE GLOBAL, at 7 (2020) https://assets.ctfassets.net/puoqjhq4x55s/4oJkKKLs0Zo43btx0t2HaO/7e72188e4eb9ae14c0b92f0290ba5a81/Advertising_in_2030_FINAL_4.28.20.pdf.

43. *See id.* at 13-14.

44. *See* Elizabeth M. Walker, *Biometric Boom: How the Private Sector Commodifies Human Characteristics*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 831, 841 (2015).

45. *See* J.D. Woodward, *Biometrics: Privacy's Foe or Privacy's Friend*?, 85 PROC. IEEE 1480, 1483-84 (1997), https://ieeexplore.ieee.org/document/628723 [https://perma.cc/NRL6-WWJG].

46. *See id.*

47. *See id.*

48. *See* SCOTT-DAWKINS & SYAL, *supra* note 42, at 13.

showing that particular individual's preferences and biometric characteristics innate to that individual. In a space which is largely unregulated, companies are left to operate and acquire information to provide an enhanced user experience.[49] On the other hand, a person can lose their anonymity and control over their data without even knowing that firms possess this type of accurate identifying information.

B. Statutes Governing the Protection of Biometric Information

This section provides an overview of the current federal and state legislative regimes in the United States, using the European Union's GDPR as a comparable international framework of reference. Federally, there are a small number of context-specific regulations protecting biometric information. In contrast, state legislation is more comprehensive but lacks nationwide application. This Note will analyze the current "patchwork" of state legislation in the United States governing the collection and use of biometric data from statutes in Illinois, Texas, Washington, New York, and California. At least four common components that appear in these varying state statutes serve to evaluate whether individuals are granted control and consistency in protection of their data. These components are namely how the statutes (1) define biometric identifiers, (2) define consent and use, (3) provide for enforcement of rights, and (4) provide a right to erasure once data is collected. These will be discussed in turn.

1. An International Comprehensive Framework

The GDPR is one of the most comprehensive frameworks in the world protecting individual data.[50] It promotes the idea of a "data bill of rights," which creates greater control for the individual over their own data.[51] These rights encompass the right to access, right to rectification, right to erasure, right to restriction of processing, right to data portability, and right to object.[52] The GDPR approaches data collection and processing broadly, emphasizing the control individuals should have over their data. The GDPR describes biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[53] Biometric data may be considered *sensitive information* if it reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" or if used to identify a particular individual.[54] As such, the processing of biometric information requires specific consent from the

49. *See id.*
50. Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 453 (2019).
51. Commission Regulation 2016/679, art. 12-23, 2016 O.J. (L 119) 1.
52. *Id.* at art. 15-21.
53. *Id.* at art. 4(14).
54. *Id.* at art. 9(1).

individual,[55] subject to some exceptions.[56] Consent is to be (1) freely given, (2) specific, (3) unambiguous of the person's wishes, and (4) must be accompanied by an affirmative act that notes their agreement.[57] All other rights such as access, complaint, correction, and erasure still apply to processors of biometric information.[58] This is a very high threshold for consent and high caliber of rights afforded to individuals within the European territory, even requiring companies which are not physically located in Europe to consistently apply these principles.[59]

2. Federal Legislation in The United States

The federal system in the United States addresses data privacy in a variety of statutes that tangentially address biometrics through a sectoral framework. These various statutes confer fewer protections on individuals by "sector," only addressing biometric information in certain contexts or for specific institutions, as opposed to broad protections issued to the general public when faced with commercial sector collection and usage. Several different statutes govern biometric data within the context of the information collected by health and medical providers,[60] the information provided to banks and financial institutions,[61] information stored by federal agencies,[62] and the protection of data collected by consumer reporting agencies.[63] This sectoral framework leaves many areas of the private and commercial use of biometric data unprotected because the statutes apply to certain institutions

55. *Id*. at art. 9(2)(a).

56. *Id.* at art. 9(2)(h). These exceptions are for diagnosis of medical conditions or to provide governmental services, amongst others.

57. *Id.* at art. 4(11).

58. *See* Dixon, *supra* note 20, at 550.

59. *See* Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 3- Consent*, INT'L ASS'N PRIV. PROS. (Jan. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/ [https://perma.cc/7JB9-WAUF]; Andrew McStay, *Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy*, BIG DATA & SOC'Y, Jan.–June 2020, at 1, 5, https://journals.sagepub.com/doi/full/10.1177/2053951720904386; *see* Dixon, *supra* note 20, at 548-49.

60. *See generally* Health Insurance Policy and Accounting Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936. Governs the collection, use, and disclosure of sensitive patient information, including biometric information only in the context of health and medical providers. *Id.*

61. *See generally* Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6802. Governs "personally identifiable financial information" provided to, resulting from a transaction, or otherwise obtained by banks and financial institutions, which can now cover some biometric information. 15 U.S.C.A. § 6809(4)(a).

62. Privacy Act of 1974, 5 U.S.C.A § 552a(a). The Privacy Act of 1974 governs how the government collects and retains information stored by federal agencies, where individuals can seek to access and amend their records. 5 U.S.C.A § 552a(d)(1).

63. Fair Credit Reporting Act (FCRA), 15 U.S.C.A. § 1681. The FCRA is responsible for the protection of data collected by consumer reporting agencies, like tenant services, credit unions, and medical information companies. The information can only be used for a specific permissible purpose in reporting to agencies, thus attaching to those purposes' legal obligations. The FCRA can encompass biometric information, as it can include information of a person's character or mode of living. 15 U.S.C.A. § 1681a, a(d)(1), b.

alone or only in specific circumstances. Early in 2020, the bill "National Biometric Information Privacy Act of 2020", which was almost an exact copy of the Illinois Biometric Information Act,[64] was introduced in the Senate. The discussion below will explain how the protections presented within the Illinois Biometric Information Act are inadequate on their own to serve as a model for a federal statute.

3. State Legislative Framework in the United States

The current patchwork of state statutes in the United States governing the collection and use of biometric data analyzed in this paper consist of laws from Illinois, Texas, Washington, New York, and California. The Illinois Biometric Information Privacy Act (BIPA) of 2008 was the first biometric information regulation passed in the United States.[65] A bill to amend BIPA is currently under review by the Illinois Legislature.[66] The Texas Capture or Use of Biometric Identifier (CUBI) of 2010 closely followed the enactment of BIPA.[67] Washington's Biometric Privacy Act (WBPA) of 2017[68] and New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) of 2020[69] were enacted almost ten years after Illinois crafted the United States' first biometric legislation. The SHIELD Act is a more comprehensive framework to protect information—including biometrics—against data breaches and unwanted disclosures, but it is not targeted towards the collection of biometric information per se.[70] The California Consumer Privacy Act (CCPA) of 2018 is arguably the most comprehensive set of data laws in the United States that grant consumers protection over their biometric information.[71] In 2020, many states attempted to pass their biometric

64. National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020) (pending on Senate Judiciary Committee), https://www.congress.gov/bill/116th-congress/senate-bill/4400/text; *compare id. with* Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. ANN. 14/1 (West 2021).

65. Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. ANN. 14/1 (West 2021); Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, THE NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 [https://perma.cc/7BSQ-PX68].

66. H.B. 559, 102d Gen. Assemb., Reg. Sess. (Ill. 2021) (to be enacted within 14/20)).

67. Capture or Use Biometric Identifier Act (CUBI), TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).

68. Washington Biometric Privacy Act (WBPA), WASH. REV. CODE ANN. § 19.375 (West 2021).

69. Stop Hacks and Improve Electronic Data Security (SHIELD) Act, N.Y. GEN. BUS. LAW § 899-aa (McKinney 2021).

70. *See id.*

71. California Consumer Privacy Act (CCPA), CAL. CIV. CODE § 1798 (West 2021).

legislation laws but failed,[72] while others have stalled their proposed legislation.[73] Other states incorporate biometric information into already existing privacy statutes.[74] The mechanics of these five statutes will be illustrated by assessing how these five different statutes implement the four following components: (1) definitions of biometric identifiers, (2) consent and use, (3) enforcement of rights, and (4) the right to erasure once data is collected, as a tool to analyze their effectiveness in providing individual control and protection to avoid a fragmented regime in the future.

a. Definitions of Biometric Identifiers

Definitions of biometric information within statutes provide the basis for what companies can and cannot extract for the purpose of creating templates within their biometric systems.[75] It delineates which information is protected and which is not protected by statute. These definitions range from narrow to broad, where broader definitions protect more individual data. BIPA attempts to define biometric information broadly, encompassing any information collected if it may be used to identify an individual. However, a "biometric identifier" is limited to "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[76] Physical characteristics and photographs are expressly excluded from these predetermined biometric

72. In 2020, states including Arizona, Maryland, New Hampshire, South Carolina, and West Virginia attempted to pass their own biometric legislation laws but failed. *See* H.B. 2728, 54th Leg., 2d Reg. Sess. (Ariz. 2020); H.B. 307, 2020, Reg. Sess. (Md. 2020); H.B. 1417, 2020, Reg. Sess. (N.H. 2020); H.B. 4812, 2020 Gen. Assemb., 123rd Sess. (S.C. 2020); H.B. 4106, 2020, Reg. Sess. (W. Va. 2020); Alicia Baiardo & Anthony Le, McGuireWoods LLP, *U.S. Biometrics Laws Part I: An Overview of 2020*, JDSUPRA (Feb. 1, 2021), https://www.jdsupra.com/legalnews/u-s-biometrics-laws-part-i-an-overview-2275684/ [https://perma.cc/4QV5-MASG]. States like Michigan, Alaska, Delaware, Florida, Montana and Rhode Island proposed bills since 2017 that also failed to go into enactment. *See* Kristine Argentine & Paul Yovanic, Seyfarth Shaw LLP, *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*, JDSUPRA (June 9, 2020), https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/ [https://perma.cc/U6KP-WCF3].

73. *See* S. No. 120, 191st Leg., 2019-2020 Sess. (Ma. 2019) https://malegislature.gov/Bills/191/SD341; Peter J. Guffin & Melanie A. Conroy, Pierce Atwood LLP, *The Massachusetts Legislature Hits the Pause Button on Comprehensive Consumer Data Privacy*, THE NAT'L L. REV. (Feb. 7, 2020) https://www.natlawreview.com/article/massachusetts-legislature-hits-pause-button-comprehensive-consumer-data-privacy [https://perma.cc/L8W7-MZAF]; Christopher G. Ward and Kelsey C. Boehm, *Developments in Biometric Information Privacy Laws*, FOLEY & LARDNER LLP (June 17, 2021), https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws [https://perma.cc/556B-CWMC}.

74. *See* Ward and Boehm, *supra* note 73.

75. *See supra* Part I.

76. TEX. BUS. & COM. CODE ANN. § 503 (West 2021).

identifiers.[77] Due to a flood of BIPA litigation,[78] the proposed new definition will be narrower; it will also exclude "information derived from biometric information that cannot be used to recreate the original biometric identifier."[79] There is available technology that allows a biometric feature to be extracted into a unique set of numbers, preventing biometric data itself from being stored.[80] Texas' CUBI has substantially the same explicit definition of a biometric identifier as BIPA, limiting the definition to "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[81]

The WBPA defines biometric identifiers more broadly than BIPA and CUBI, subject to a specific set of exceptions. Its definition includes "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 . . . [yet] . . . does not include a physical or digital photograph, video or audio recording or data generated therefrom . . . ."[82] By explicitly excluding physical or digital photographs and failing to include facial geometry as a biological characteristic,[83] WBPA has a narrow set of identifiers that fall within the purview of the statute.

New York's SHIELD Act defines biometric identifiers as "data generated by electronic measurements of an individual's unique physical characteristics, such as […] a fingerprint, voice print, retina or iris image, […] or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity."[84] This definition targets any information considered "extractable" and capable of ascertaining an individual's identity, thus making it broader than the other statutes combined. Lastly, the CCPA defines biometric information as an "individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, *singly or in combination* with each other or with other identifying data, to establish individual identity."[85] This definition is the broadest and least exclusive statutory definition by its terms, and is possibly capable of including future technologies that can lead to the identification of an individual.[86]

---

77. *Id.* "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."

78. Kwabena A. Appenteng & Andrew Gray, *Illinois Legislature Considers a Bill Designed to Slow the Flood of Biometric Privacy Class Action*, LITTLER (Mar. 15, 2021), https://www.littler.com/publication-press/publication/illinois-legislature-considers-bill-designed-slow-flood-biometric [https://perma.cc/D6P7-7QM2].

79. H.B. 559, 102d Gen. Assemb., Reg. Sess. (Ill. 2021) (to be enacted within 14/15(b)(3)).

80. *See* Appenteng & Gray, *supra* note 78.

81. TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2021).

82. WASH. REV. CODE ANN. § 19.375.010(1) (West 2021).

83. *Id.*

84. N.Y. GEN. BUS. LAW § 899-aa(b)(5) (McKinney 2021).

85. CAL. CIV. CODE § 1798.140(c) (West 2021) (emphasis added).

86. *Id.*

Cases brought under BIPA have challenged the statutory definitions of biometric identifiers. Two particularly instructive cases are *Rivera v. Google* and *Patel v. Facebook.* In *Rivera*, plaintiffs alleged that Google scanned their facial geometry in violation of BIPA, using photos uploaded to a friend's Google Photos application.[87] Google responded that plaintiffs did not have a sufficient claim and that they were in violation of BIPA because photographs and their derivative information were explicitly excluded from the statutory definition.[88] Ultimately, the court did not resolve the issue of scanning facial geometry as the case was dismissed for lack of Article III standing, which will be discussed below.[89] Similarly, in *Patel*, plaintiffs alleged that the "tag" feature used by Facebook was unlawfully collecting their facial geometry without consent from uploaded photographs.[90] Facebook, like Google in *Rivera v. Google, Inc*, moved to dismiss the class-action suit based on lack of Article III standing for failing to state a concrete injury.[91] In contrast with the *Rivera* decision, the Ninth Circuit in *Patel* decided that plaintiff's claims were actionable, viewing unconsented collection as an actionable injury.[92] Although the Supreme Court allowed the suit to continue by denying certiorari,[93] Facebook eventually announced its intention to settle the suit for $550 million,[94] leaving the question of how facial geometry could be extractable from photographs that are expressly excluded as biometric identifiers under BIPA's statutory definition unresolved.

b. Consent To Collect and Sell Biometric Information

Data privacy legislation relied on including biometric information in their definitions, focusing on unauthorized disclosures or misuse of collected data.[95] Recent years shifted the focus towards how data itself is collected from individuals and used regularly with or without their knowledge. Most of the legislation tackling biometric regulation, except for the CCPA,[96] focuses on requiring some type of consent from the user before collecting the user's information, because, in theory, it grants consumers autonomy over the

87. *See* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1001 (N.D. Ill. 2018).
88. *See* Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1092 (N.D. Ill. 2017).
89. *See Rivera*, 366 F. Supp. 3d at 1001.
90. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019).
91. *See id.* at 1269.
92. *See id.* at 1275.
93. *See* Patel v. Facebook, Inc., 932 F.3d 1264, *cert. denied.* 140 S. Ct. 937 (2020). Facebook appealed the decision to Supreme Court, but it was denied.
94. *See* Rachel Pester, *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit*, JOLT DIGEST (Feb. 14, 2020), https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit [https://perma.cc/BJU6-2VD5].
95. Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, BUS. L. TODAY, May 20, 2016, at 1, 4.
96. CAL. CIV. CODE § 1798.100(a)-(e) (West 2021).

release of their data.[97] However, some states require informed consent, others require a context-dependent consent, and in states without legislation, no consent is required for collection or sale unless included within a broader privacy regime.[98] These inconsistencies provide a lack of control for individuals and do not provide a solid ground upon which companies can operate under.

BIPA requires informed consent from consumers before a company collects information, requiring that individuals be informed of the specific purpose for the collection, length of time the information will be stored, and provide a written release of the information.[99] Similarly, BIPA prohibits the sale of data for commercial gain and disclosure of the information without the user's consent or as mandated by court order or federal law.[100] Taking after BIPA, CUBI prohibits the collection of biometric information for a commercial purpose unless the person provides informed consent, as well as prohibits disclosure of the collected information subject to similar exceptions.[101] The WBPA also does not allow the collection of biometric information in a commercial database without first obtaining consent from the individual or without providing "an alternate mechanism to prevent subsequent use" of the information for commercial purposes.[102] However, WBPA notes that consent is context-dependent, thus it has more relaxed requirements than BIPA.[103]

In contrast, the CCPA does not require consent. Individuals have a right to know what information is being collected, the purpose of collection, and the disclosures being made.[104] Instead of consent, they are given the choice to opt-out from their information being sold and shared with third parties.[105]

c. Enforcement Rights

The two enforcement rights in these statutes are the private right of action and actions brought forth by the Attorney General. BIPA uniquely

---

97. *See* Daniel J. Solove, *Introduction: Priva Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1879, 1892 (2013); *see also* WOODROW HARTZOG, *BIPA: The Most Important Biometric Privacy Law in the US?*, REGULATING BIOMETRICS GLOB. APPROACHES & URGENT QUESTIONS, Sept. 2020, at 96, 102-103, https://ainowinstitute.org/regulatingbiometrics.pdf.

98. Illinois and Texas require informed consent. 740 ILL. COMP. STAT. ANN. 14/15(b)(1)-(3) (West 2021); TEX. BUS. & COM. CODE ANN. § 503.001(b)-(c) (West 2021). Washington requires a context dependent consent. WASH. REV. CODE ANN. § 19.375.020(2) (West 2021); *see* Claypoole & Stoll, *supra* note 95.

99. 14/15(b)(1)-(3) (Westlaw). The release will be "written consent" instead of "written release" and may be obtained in electronic form. H.B. 559, 102d Gen. Assemb., Reg. Sess. (Ill. 2021) (to be enacted within 14/15(b)(3)).

100. 14/15(b)-(d) (Westlaw).

101. BUS. & COM. § 503.001(b)-(c) (Westlaw). Exceptions include to serve as an identifier in the event of death, to complete a financial transaction requested by the individual, or as mandated by federal or state law.

102. § 19.375.020(1) (Westlaw).

103. § 19.375.020(2) (Westlaw).

104. CAL. CIV. CODE § 1798.100(a)-(e) (West 2021).

105. CIV. §§ 1798.100(a)-(b), .105(b), .110, .115, .120(a)-(b), .130, .135 (Westlaw).

contains a private right of action for persons "aggrieved by a violation" of the statute subject to monetary penalties.[106] However, the proposed legislation may eradicate the right of action by adding a one-year statute of limitations, adding a 30 day cure period for violations.[107] In addition, the Illinois legislature attempts to restrict the damages previously imposed on violators of the act to only actual damages and erasing statutory damages from the provisions.[108] The CCPA also provides a private right of action against those companies that do not take appropriate measures to protect collected data. [109] This limited private right of action is only for "nonencrypted and nonredacted personal information . . . subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures . . . ."[110] Essentially, this right is only for security breaches, as opposed to the collection and misuse of information itself that is unique to BIPA's provision.[111] The three remaining statutes, CUBI,[112] WBPA,[113] and the SHIELD Act[114] only allow the Attorney General to take enforceable action, which includes monetary penalties.[115] Consumers do not possess the autonomy to sue for statutory violations under these frameworks.

The cases of *Rivera* and *Patel* also demonstrate how a claim brought under BIPA faces challenges in federal court if brought as a class action when individuals try to assert control over their data. In both *Rivera* and *Patel*, the defendant corporations challenged the class action suits under Article III standing for lack of a concrete injury, [116] which is required for a claim to possess Article III standing.[117] In *Spokeo v. Robins* (Spokeo I), the Supreme Court identified that Article III standing may exist where (1) statutory violations are closely related to harms traditionally recognized or (2) Congress indicates for intangible harm to be considered concrete within the privacy sector.[118] A mere procedural violation of the statute is insufficient

106. 740 ILL. COMP. STAT. ANN. 14/20(1)-(2) (West 2021). A negligent violation is for 1,000 dollars and intentional or reckless violations are for 5,000 dollars for each violation of the statute.

107. H.B. 559 102d Gen. Assemb., Reg. Sess. (Ill. 2021) (to be enacted within 14/20).

108. *Id.*

109. CIV. § 1798.150(a)(1) (Westlaw) (as amended by Assemb. B. 1355, 2019 Gen. Assemb., Reg. Sess. (Cal. 2019)).

110. *Id.*

111. 14/20.

112. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2021).

113. WASH. REV. CODE § 19.86.140 (West 2021).

114. N.Y. GEN. BUS. LAW § 899-aa(6)(a) (McKinney 2021).

115. BUS. & COM. § 503.001(d) (Westlaw). The penalties for violations of CUBI are for 25,000 dollars in damages for each violation; § 19.375.030. WBPA penalties range from 2,000 dollars per violation. The Washington Legislature considered the Washington Biometric Protection Act as unfair and deceptive practices under Section 19.86.020, thus covered and actionable under Section 19.86.140.

116. *See* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1001 (N.D. Ill. 2018); *see* Patel v. Facebook, Inc., 932 F.3d 1264, 1269 (9th Cir. 2019).

117. *See* Michelle Jackson, *Opting Out: Biometric Information Privacy and Standing*, 18 DUKE L. & TECHNOLOGY REV. 293, 297 (2020); Spokeo, Inc. v. Robins (*Spokeo I*), 136 S. Ct. 1540, 1549 (2016).

118. *Spokeo I*, 136 S. Ct. at 1548-49.

absent some showing that there is a risk of harm or an invasion of a legally protected interest uniquely identified by Congress.[119] The Supreme Court, however, recently took a decisive stance that "Congress's creation of statutory violation or obligation and a cause of action" doesn't automatically grant relief without meeting the concrete injury requirement.[120] This is particularly challenging for privacy claims.

Privacy cases face challenges in defining what harm is suffered when information is collected absent some risk of disclosure or unauthorized access by third parties (i.e., entities other than the company). In essence, courts were asked to analyze whether the unauthorized collection and creation of the facial templates were truly a "harm" or posed a risk of harm,[121] as this can be interpreted as a loss of an individual's anonymity through biometric identification. In *Patel*, the right to the individual's privacy interests required no additional injury besides the violation of the statute itself.[122] In contrast, the Illinois Northern District Court that sits within the Seventh Circuit in *Rivera* held that a statutory violation of BIPA for unconsented collection of biometric information was insufficient to gain Article III standing without further risk of disclosure. [123] The harm defined, as interpreted by the court, was disclosure and identity theft instead of a right to privacy.[124] The Seventh Circuit in a later case *Bryant v. Compass Group*, however, opined that the unconsented collection of fingerprints – a protected biometric identifier by statute – sufficed the Article III requirement.[125]

The disagreement amongst various courts in defining the privacy harms suffered by individuals demonstrates a problem in using the statute to exercise rights granted to individuals. If courts do not regard these harms as concrete, individuals are left with little recourse to control their information because companies can invoke Article III to stop the suits[126] and continue with their regular practices.

d. Right to Erasure

No state statute other than the CCPA provides the right to erase information upon an individual's request and force companies to direct their service providers to do the same.[127] CUBI similarly mandates deletion of collected information after one year of collection.[128] However, BIPA, CUBI, and WBPA do not provide this right to individuals whose information has

119. *Id.*
120. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2205 (2021).
121. *See Patel*, 932 F.3d at 1273.
122. *See id.* at 1275.
123. *See* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1010, 1012-14 (N.D. Ill. 2018).
124. *Id.*
125. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020).
126. *See id.* at 1001.
127. CAL. CIV. CODE § 1798.105(a) (West 2021). Exemptions found in § 1798.105(d).
128. TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (West 2021).

been collected by commercial firms. This right is foundational in the GDPR.[129]

III. ANALYSIS

A. *Inadequacies In Current Biometric Regimes in the United States*

The current patchwork of legislation in the United States regarding the collection and use of biometric data is inadequate for both consumers and corporations due to the inconsistencies in legislation across states that do afford some protection. Each regime provides a different set of requirements. In states where no law is enacted, biometric information remains free to collect, sell, and use. This section argues that narrow definitions of biometric identifiers, the consent system value-exchange, the private right of action's definition of harm, and the lack of a right to erasure are obstacles in providing individuals control over their data and create inconsistent expectations of compliance for companies operating in this space.

1. Narrow Definitions of "Biometric Identifiers" Create Inconsistent Protection Across States and Do Not Account for The Rapid Growth of Biometric Identification Technology

Different statutes across the United States provide varying definitions of biometric identifiers. This lack of uniformity fails to protect individuals consistently and fails to consider how new technology will render statutes easily outdated. Narrowly defining biometric identifiers changes what corporations in one jurisdiction can consider extractable information to create templates for biometric systems and makes those non-extractable features protected by statute.[130] The narrow and broad definitions in the different statutes leave individuals protected to varying degrees across states.

Narrowly defining biometric identifiers and their exclusions limits an individual's control and protection granted by statute. Individuals in Illinois and Texas are only protected from the unconsented collection of "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry,"[131] in contrast to Washington, New York, and California residents who have protection from the collection of "other unique biological characteristics" that may be used to establish individual identity.[132] The exclusions from the statutory definitions in BIPA, CUBI, and WCPA[133] can run contrary to the aims of the legislators when enacting these protections. For example, the

129. Commission Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43.

130. *See supra* Part I(a).

131. BUS. & COM. § 503.001(a) (Westlaw).

132. WASH. REV. CODE ANN. § 19.375.010(1) (West 2021); N.Y. GEN. BUS. LAW § 899-aa(5)(5) (McKinney 2021); CIV. § 1798.140(b) (Westlaw).

133. *See supra* Part II(c)(1).

exclusion of "photographs . . . or physical descriptions . . . such as height, weight, hair color, or eye color" in BIPA, runs contrary to other sections of the statute that define biometric information as "any information[,] regardless of how it is captured" used for identification purposes.[134] BIPA's legislative intent section notes that there should be greater protection because "biometrics . . . are biologically unique to the individual" and its "ramifications . . . are not fully known."[135] Under the current system, however, there is no obstacle for companies attempting to extract facial templates from photographs in Illinois, Texas, and Washington, even if they include facial geometry.[136] On the other hand, firms would be unable to do so in California or New York because there is no explicit photograph exclusion.[137] These inconsistencies shift control to the companies, as opposed to individuals whose data is at issue when collecting and using information for personalized customer experiences.[138]

A narrow definition approach of extractable sources of biometric data also does not encompass the development of technology in this field. Today, there is more development of biometric measurements, such as cardiac rhythm to behavioral biometrics, as collective traits that can be placed together to form an identity.[139] Turning back to my hypothetical at the beginning of this Note, there may be a future where advertisers are not only tracking a viewer's eye movements[140] but would like to gain access to a combination of metrics available through novel technology, such as combining ECG and EEGs, [141] to identify a particular consumers' reaction to an advertising campaign. This lack of breadth was demonstrated in *Rivera* and *Patel*, which were brought under BIPA, where plaintiffs alleged that the unconsented collection of facial geometry extracted from photographs was a violation of the statute.[142] The lack of clarity surrounding whether the mapping facial geometry from photographs (that is not protected under BIPA) is a violation of BIPA demonstrates how technological advances pose challenges to protecting information.

In contrast, New York's SHIELD, California's CCPA, and the GDPR include broader definitions that can encompass future technologies that may be used for identification collectively. The CCPA's broad definition of an "individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, *singly or in combination* with each other or with other identifying data, to establish individual identity"[143] is non-exclusive, better reflecting the evolvement of the technology. Broadening the definitions of biometric data

134. 740 ILL. COMP. STAT. ANN. 14/1 (West 2021).
135. 14/05(c), (f) (Westlaw).
136. *See generally* 14; BUS. & COM. § 503.001 (Westlaw); § 19.375.010 (Westlaw).
137. GEN. BUS. § 899-aa(5)(5); CIV. § 1798.140(c).
138. *See generally* SCOTT-DAWKINS & SYAL, *supra* note 42, at 13.
139. *See* Palaniappan et al., *supra* note 10, at 177, 184; Roberg-Perez, *supra* note 9.
140. *See* Hood, *supra* note 36.
141. *See* Palaniappan et al., *supra* note 10, at 177, 184.
142. *See* Rivera v. Google, Inc., 366 F. Supp. 3d, 998, 1001 (N.D. Ill. 2018); *see* Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019).
143. CAL. CIV. CODE § 1798.140(c) (West 2021) (emphasis added).

affords greater and consistent protection, allowing the statute to remain up to date as novel means of extracting information become available.

2. The Consent System's Value Exchange Does Not Provide Control to Consumers

A requirement that individuals provide informed consent in BIPA[144] and CUBI,[145] and the more relaxed consent-based system in WCPA,[146] should theoretically provide individuals with greater control over what data is being collected and sold. Nevertheless, the consent system is rendered less effective when individuals exchange their data for services, thresholds for consent are easily cleared, and no remedy exists for data collected before a consent-based system was imposed.

While explicit consent is designed to prevent companies from collecting data without the individual's permission, it is not widely known whether or not most individuals would choose to opt-in to services by exchanging data.[147] A problem exists because individuals are likely to consent in order to use certain features of services. If you want to use the Bank of America app that requires fingerprinting, you are likely to consent in order to reap the benefits of this unique feature and maintain your information security. Likewise, individuals with iPhones are likely to register their Face ID with Apple in order to unlock their phones by holding them up to their faces. This type of use renders consent an ineffective tool because as Professor Woodrow Hartzog argues, the promulgation of risk is offloaded to consumers as opposed to the data collectors.[148] This is echoed by Ruth Gavison in the Yale Law Journal, noting that focusing responsibility on people's choices fails to acknowledge privacy as a stand-alone concept to be respected by others unless one chooses to exercise release of said privacy.[149] If consumers easily consent for services, statutory protection of consent does not provide much autonomy to the individual unless they choose to opt-out of the service as a whole.

Even where a consumer is not required to consent, like in the CCPA, an opt-out right from data being sold to third parties[150] as well as proposition 24's opt-out of data sharing,[151] do not stop companies from leveraging data over services that create a value exchange for the consumer. Firms may offer financial incentives through the CCPA in "different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data."[152] While this approach promotes a value exchange for the consumer,

144. 740 ILL. COMP. STAT. ANN. 14/15 (b)(1)(3) (West 2021).
145. TEX. BUS. & COM. CODE ANN. § 503.001(b)-(c) (West 2021).
146. WASH. REV. CODE ANN. § 19.375.020(2) (West 2021).
147. *See* SCOTT-DAWKINS & SYAL, *supra* note 42; EMARKETER, *supra* note 39.
148. *See* HARTZOG, *supra* note 97, at 102-03.
149. *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421, 427 (1980).
150. CAL. CIV. CODE § 1798.120(a) (West 2021).
151. *Id.*
152. *Id.* § 1798.125(b)(1) (Westlaw).

thereby increasing control, both a strict consent system and opt-out system allow companies to dangle incentives for individuals to release their data, undermining the individual's control.

Second, the threshold for defining "consent" is extremely low where consent is given in exchange for services. Cases under BIPA, which requires express and written release, have found consent to be freely given in certain circumstances. In a case brought under BIPA, lockers were assigned to customers after they scanned their fingerprints into a fingerprint scanner; the locker numbers that customers were given corresponded to their digital fingerprint as their lock.[153] The court found that the customers did give consent because they expected that the data would be retained for the duration of the rental due to the design of the system.[154] Similarly, in a Second Circuit case, a basketball video game allowed players to recreate themselves as an avatar by scanning their faces into the system.[155] All players needed was to click a "continue button" in order to record the scan.[156] The Second Circuit held that the defendant's video game had satisfied BIPA's notice and consent provisions and that there was no risk of harm.[157] If the strongest form of consent like BIPA's is easily bypassed, individuals in states with context-dependent requirements face an even lower bar, rendering this tool ineffective for the purpose of protecting unsuspecting consumers.

Third, the system does not address the data already collected and processed without users' knowledge and before any regimes were put in place. If a grocery store collected your facial template without your knowledge, a consent-based system becomes a stronger argument to show that the store possessed no rights to collect said information. However, if the store already collected this information, the system is palpably weak when viewed retroactively, as argued by Professor Hartzog, because there is no recourse for a consumer that is not aware that their data was collected.[158]

While the BIPA, CUBI, and WBPA regimes are very different than the CCPA, the protections can fail under all of these regimes. If in some states you would likely consent to use a service and in others you could trade in data for a better type of service, consent or opt-out remains an ineffective tool to truly provide individuals with autonomy over their data. For the average person that needs to use technology or access a feature, there is little to motivate them from not consenting if they benefit or receive a reward in exchange.

153. *See* McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 U.S. Dist. LEXIS 100404, at *7 (N.D. Ill. Aug. 1, 2016).

154. *Id.*

155. *See* Santana v. Take-Two Interactive Software, Inc., No. 17-303, 2017 U.S. App. LEXIS 23446, at *1 (2d Cir. Nov. 21, 2017).

156. *Id.*

157. *Id.* at *3.

158. *See* HARTZOG, *supra* note 97.

3. Force of The Right to Private Action Is Diminished by Article III Standing Challenges

The protection offered by a private right of action for individuals to control their information is diminished because courts can inconsistently interpret what constitutes a "harm" within the "concrete injury requirement." This is demonstrated by the split in circuits over BIPA claims in federal class-action suits; the Ninth Circuit in *Patel* ruled that the violation of the statute was sufficient, but the Illinois Northern District Court within the Seventh Circuit in *Rivera* went in the opposite direction just a year earlier.[159] Michael Rivera, writing for the *Fordham Intellectual Property, Media and Entertainment Law Journal*, proposed that the private right of action was the best remedy to provide consumers with protection over their data from ambitious firms.[160] While in theory, the right exists, its application remains inconsistent to provide sufficient protection as the best remedy, at least as currently enacted.

The Ninth Circuit in *Patel v. Facebook* adopted a similar line of reasoning to the Supreme Court of Illinois in *Rosenbach v. Six Flags* that a "violation [of BIPA], in itself, is sufficient to support the individual's or customer's statutory cause of action."[161] The Ninth Circuit noted that for purposes of Article III standing, intangible harms such as "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact" without the need to state additional harms.[162] This is true so long as the provision meets the aforementioned criteria to protect concrete interests and there is an indication the harm was to be protected.[163] The *Patel* Court, in analyzing the text of BIPA as a whole, decided that the Illinois legislature had codified a right to privacy in personal biometric information.[164] The procedural protections written into the legislation thus afforded the individual this right to privacy.[165] Failure to follow the procedural requirements of the statute made it so the plaintiffs' rights "would vanish into thin air" and the harm to be prevented became true.[166] Furthermore, the court noted these harms were traditionally seen in common law as an invasion of privacy, and therefore sufficient to withstand the motion to dismiss.[167]

The District Court in *Rivera* used both history and Congress's judgment as the backdrop of its interpretation, emphasizing that a procedural violation

159. *Compare* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1010, 1012-14 (N.D. Ill. 2018), *with* Patel v. Facebook, Inc., 932 F.3d 1264, 1275 (9th Cir. 2019).

160. Michael A. Rivera, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 571, 597-603 (2019).

161. *See* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).

162. *See Patel*, 290 F. Supp. 3d at 952 (quoting Spokeo, Inc. v. Robins (*Spokeo I*), 136 S. Ct. 1540, 1549 (2016)).

163. *Id.* at 953.

164. *Id.*

165. *Id.*at 954.

166. *Id.*

167. *Id.*

could be sufficient if the risk of harm was sufficiently concrete.[168] In its view, however, the plaintiffs did not allege "injury" beyond being merely "upset" or "angry" that the photos were out of their control.[169] The court relied on a line of cases where Article III standing was only conferred where there was a lack of consent and subsequent unconsented disclosure.[170] By defining the harm differently, or put simply, viewing the unconsented collection of facial geometry without future risk of disclosure as insufficient as a harm, it found that there was no risk of harm nor an intrusion of privacy on the individual.[171] The court disagreed strongly with *Patel*'s "across-the-board conclusion that all cases involving any private entity that collects or retains individuals' biometric data present a sufficient risk of disclosure that concrete injury has been satisfied in every case."[172] The court went further to state that the general conclusions of the Illinois legislature protecting biometric data because of its "public welfare, security, and safety will be served"[173] were too general.[174] As people expose their faces to the public every day, that information is more widely public than a social security number,[175] thus rejecting plaintiffs' arguments that their faces when codified into biometric templates should be considered private.[176] It found that "[a]ll Google did was to create a face template based on otherwise public information" and that such an act was not highly offensive as an intrusion.[177]

This disjunctive interpretation of what rises to be a "privacy harm" creates a lack of parity for individuals seeking to enforce their rights and for companies seeking to follow procedural requirements of the statute, which would force compliance with the provisions because of the threat of suits. If the collection of an individuals' information is not seen as real harm, even if the state courts do recognize this right to privacy as seen in *Six Flags,* the derogation in federal courts diminishes the protection afforded by statute.

Moreover, the recent Supreme Court decision in *TransUnion v. Ramirez* further emphasizes how the Supreme court is also strict in its application of the concrete injury requirement in privacy harms. The Court notes that merely having a statutory cause of action made available by Congress, absent a serious likelihood of disclosure,[178] does not bypass the requirement that the plaintiff suffer a concrete injury that satisfies the court's

168. *See* Rivera v. Google, Inc.,366 F. Supp. 3d 998, 1004 (N.D. Ill. 2018) (citing Spokeo, Inc. v. Robins (*Spokeo I*), 136 S. Ct. 1540, 1549 (2016)).

169. *Id.* at 1007-08.

170. *Id.* at 1009 (citing Miller v. Southwest Airlines Co., No. 18 C 86, 2018 U.S. Dist. LEXIS 143369, at *3 (N.D. Ill. Aug. 23, 2018); Dixon v. Washington & Jane Smith Cmty.-Beverly, No. 17 C 8033, 2018 U.S. Dist. LEXIS 90344, at *10 (N.D. Ill. May 31, 2018)).

171. *Id.*

172. *Id.* at 1010.

173. 740 ILL. COMP. STAT. ANN. 14/5(f), (g) (West 2021).

174. *See Rivera*, 366 F. Supp. 3d at 1010-11.

175. *Id.*

176. *Id.* at 1012 (explaining that an expectation of privacy in a person's face in public is inconsistent with the Fourth Amendment's expectation of privacy).

177. *Id.* at 1012-13.

178. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2212 (2021).

interpretation.[179] While distinguishable from the context of biometric privacy concerns, the Court does not bring much hope that privacy harms per se will be considered injuries. Since the *Six Flags* case was decided after *Rivera*, there is some hope that future cases decided by the circuits, as done so by *Bryant*, may bring about uniformity in applying the private right of action in diversity suits.[180]

The CCPA's limited right of action, focused on breaches and cure of said breaches[181] will be subject to scrutiny for claims based on the failure to provide notice and opt-outs before sharing information with third parties because it falls outside the language of § 1798.150(c.)[182] This is conditioned by the ability of businesses to cure the defect to cease the action.[183] However, this right is centered on a more concrete harm of disclosure and thus is less likely to face the same challenges as the nebulous concept of the "right to privacy" under BIPA.

4. The Right of Erasure Provides Greater Autonomy to Individuals Over Their Data

The right to erasure provides individuals greater agency over their data once they no longer consent to the processing of their data, or never consented to the collection of their data to begin with.[184] Due to the infeasibility of obtaining proper consent from individuals, erasure provides a stronger mechanism for individuals to remain in control. Only the CCPA in the United States, following the GDPR model, provides this right.[185] The CUBI one year provision is more of an automatic deletion by the collecting entity.[186]

This right is important because humans have long had the practice of forgetting within our systems of memory.[187] The judicial system also provides for this kind of forgetting so people may begin new lives or not be judged by

179. *Id.* at 2205.

180. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020).

181. CAL. CIV. CODE § 1798.150(a)-(b) (West 2021).

182. *See* Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, INT'L ASS'N OF PRIV. PROS. (June 8, 2020), https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/ [https://perma.cc/R9HB-6K3Y]; CIV. § 1798.150(c) ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title.").

183. CIV. § 1798.150(b) (Westlaw).

184. Ben Wolford, *Everything You Need to Know About the Right to be Forgotten*, GDPR.EU, https://gdpr.eu/right-to-be-forgotten/ [https://perma.cc/LY79-C9TD].

185. CIV. § 1798.105 (Westlaw).

186. TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (West 2021).

187. *See generally* Eugenia Politou, Efthimios Alepis & Constantinos Patsakis, *Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions*, J. CYBERSECURITY Mar. 26, 2018, at 1, 9, https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056 (citing Liam J. Bannon, *Forgetting as a Feature, Not a Bug: the Duality of Memory and Implications for Ubiquitous Computing*, 2 INT'L J. COCREATION DESIGN & ARTS 1, 2-15 (2006)) [https://perma.cc/H37Q-XCM9].

the past.[188] Previously, loss of anonymity was not a concern when the world mostly operated in paper-only formats, because it was impossible to truly centralize the entire system.[189] The default in the past was forgetting, whereas today the roles are inverted and forgetting is the exception.[190] This inability to forget, especially with sensitive information uniquely capable of identifying you, contributes to the invasion into daily life at the core of the biometric privacy debate.[191] No data point goes unnoticed, recreating the digital version of an individual to perfection if it includes the unique biometric data that only belongs to that one individual. Without reparations in courts or a consent system that is not operating as a value-exchange, the ability to erase data remains a strong method to give control over information containing features capable of identifying us more accurately than other types of data.

B. A Federal Legislative Solution

To avoid the patchwork of legislative regimes with different standards of protection for individuals, or without any at all,[192] Congress should adopt a federal law addressing these inconsistencies from the existing legislation. Taking a lessons-learned approach, the adoption of federal legislation to patch up the inadequacies of the various state regimes currently in place should borrow from existing statutes and focus on addressing the (1) definitions of biometric identifiers, (2) thresholds for consent to collect and use data, (3) enforcement mechanisms, and (4) the right to erase data collected. These four elements, as analyzed, can grant individuals greater control and provide companies a consistent framework under which to operate.

First, the proposed federal initiative should incorporate an expansive definition for biometric identifiers, like that of the CCPA and the GDPR. This definition will proactively keep the law from becoming easily outdated by the emergence of new biometric technology used to identify individuals. To provide greater individual control, one all-encompassing definition could grant individuals greater protection because it identifies all possible areas of which biometric information may be obtained. From an operational perspective, it provides a consistent guideline for companies to operate their systems. However, there is the possibility that such a law may give rise to a variety of lawsuits contesting what types of technology would fall under the statutory definition, as seen in *Rivera v. Google* and *Patel v. Facebook.* Another alternative would be to require by statute that companies use the available technology to convert a biometric identifier into a unique numbering sequence. [193] This solution would allow companies to operate without falling within the scope of the various definitions, because the information could not

188. *Id.*

189. *Id.*

190. *Id.* (citing VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (Princeton University Press, 2011)).

191. *See* Woodward, *supra* note 47.

192. For those states that do not have statutes, their citizens receive little protection.

193. *See* Appenteng & Gray, *supra* note 78.

be later used to "identify" an individual or "recreate the original biometric identifier."[194]

Second, a consent-based approach provides very little when it comes to user protection, and it varies in application across statutes. If we are to avoid overbroad collection, BIPA's or CUBI's stringent informed consent standard would be the best avenue to prevent data that is yet to be collected. Yet, the high rate of consumer consent may point Congress to adopt a standard that allows consumers to gain something if they are to be giving away their data. The approach in the CCPA would allow users to have more control once they choose to opt-out of a system and choose a value in exchange for their data. Consent, however, just like the private right of action, does not give individuals any true agency in maintaining "privacy" because it is unclear whether true consent is ever achieved. Congress should focus on the model of whether consent will be a tool to stop overbroad collection or if individuals should instead receive benefits because they have released their data.

Third, providing a private right of action federally, like BIPA, will come with a set of challenges due to Article III standing and the concrete harm requirement when it relates to intangible privacy harms, as reflected in the recent *TransUnion* Case.[195] While jurisprudence is growing in this sector and could provide some clarity, what constitutes a privacy harm will continue to provide challenges for plaintiffs to enforce their rights unless these harms are more clearly defined. If Congress were to draft a provision analogous to BIPA, it must be premised on clearly defining the harms envisioned to avoid conflicting interpretations in the courts. This action will only serve as an effective mechanism where corporations know they must adhere to the statutory provisions to avoid tremendous damages and reinstate control for individuals if they know their rights can be enforced through the courts. Of course, the possibility that courts would render conflicting interpretations from what Congress believed to be a clearly defined harm remains. What is observed in Illinois is that the legislature wishes to decrease damages in the revised statute to avoid the flood of litigation and burden placed on companies in the sector.

Lastly, a provision that should be drafted into a federal statute to grant autonomy for the individual is for access and a right to delete information. While the aforementioned elements are important, the right to erase can warrant full control to individuals over their data as a fail-safe mechanism when the other provisions do not operate effectively. A right to erasure may be the only avenue left to control how data is being harbored by firms if consent becomes superfluous, definitions become outdated, and a private right of action cannot make a plaintiff whole or force companies to abide by the statutory provisions. In this sense, the right to erase would be the last resort for the individual to be "forgotten." It is natural to question, however, how

194. H.B. 559, 102d Gen. Assemb., Reg. Sess. (Ill. 2021) (to be enacted within 740 ILL. COMP. STAT. ANN. 14/10).

195. *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2205 (2021).

often an individual would choose to exercise that statutorily granted right, if at all.

IV. CONCLUSION

The current patchwork of legislation in the United States regarding the use and collection of biometric data is inadequate due to lack of uniformity in definitions of biometric identifiers, the value-exchange offered for consent, difficulty in defining privacy harms for private rights of action, and the lack of means to erase collected data. Congress should adopt a federal law introducing unifying principles for businesses and consumers alike. From these rights, the core principle of control and the right to delete data can grant greater autonomy over individuals' uniquely sensitive biometric information that the current systems in place are failing to protect. Turning back to the not so unthinkable hypothetical posed in the Introduction of this Note, if Congress could pass federal regulation that adopted broad definitions biometric identifiers and required some consent before this type of identifiable information was collected, someone's cigarette containing DNA could not be matched with their bank's ATM footage and reconstruct their face on a billboard. Firms would not be able to freely share and match this information resulting in ad-campaigns and automatic fines for littering. Moreover, this individual would have a right to demand that the company delete information collected about them and sue if said statute recognized a private right of action with a specific privacy harm outlined. This would grant the individual much more control and provide companies with a consistent framework that sets expectations and greater obligations upon collection and use of an individual's biometric information.