A BLURRY LENS: ASSESSING THE COMPLICATED LEGAL LANDSCAPE OF BIOMETRIC PRIVACY THROUGH THE PERSPECTIVE OF MOBILE APPS

*Mackenzie K. Mendolla**

I. INTRODUCTION

The use of biometric data has become a part of today's new normal—and it is here to stay. In fact, biometric authentication is now intertwined in society's daily routine and many individuals may not have even noticed it. Most people have come to rely on this technology in ways that they may not fully comprehend at this moment. People use mobile apps for social media platforms, entertainment and television, shopping, and online banking.[1] One of the most common and well-known ways that biometric data is used on mobile apps is through identification and authentication.[2] This usage created an additional layer of protection for users that has strengthened cybersecurity[3]—but it has also caused a numbness to the ways in which people share their most personal data. Mobile apps have the potential to use biometric data outside of authentication and identification; for example, mobile apps may use biometrics to support app performance and to benefit technological platforms.[4] When biometric data is used outside of its intended and original application, consumers should be wary of whose hands the data ends up in. Consumers must be able to control their data—especially where it goes and how it is used.

In analyzing why biometrics present unique privacy risks, it is necessary to look at the nature of biometric data itself. Biometric data

* J.D. Candidate, 2024, Seton Hall University School of Law; B.A. Psychology and Public Health, *cum laude*, 2021, Boston University.

[1] Nelson Gomes, *Where Mobile Apps Benefit from Biometrics*, TECHNATIVE (Feb. 19, 2020), https://technative.io/where-mobile-apps-benefit-from-biometrics.

[2] *Id.*

[3] *See* Domenic Molinaro, *What Is Biometrics and How Secure Is Biometric Data?*, AVAST: ACADEMY (Nov. 4, 2022), https://www.avast.com/c-what-is-biometric-data (explaining that biometric security is difficult to hack due to the complex and random nature of biometric identifiers).

[4] *See infra* notes 136–43 and accompanying text.

has evolved "to include fingerprint recognition, facial recognition, voice recognition, iris recognition[,] and even finger vein recognition more recently" as a means of unlocking apps or private features on apps.[5] For example, banking and financial apps permit customers to log into their accounts using fingerprints or facial scans.[6] Authentication works like this: a user will log into their app using a specific biometric identifier (such as a fingerprint), and the identifier is then "authenticated by the backend and tied to a mobile keychain containing their password."[7]

Biometrics are measurements of an individual's physical characteristics, including fingerprints, facial data, voiceprints, retinal and iris patterns, and DNA—to name a few.[8] Biometrics can also include behavioral characteristics, such as an individual's mannerisms, a signature, or the way that an individual walks.[9] The nature of biometrics creates an area ripe for privacy risks. Data breaches put people at risk for identity theft.[10] This situation, however, is more serious than a stolen password as people are unable to change their biometrics. Biometric data can also be captured at a distance from the individual; for example, facial scans and a person's gait can be recorded from far away, leaving people with less control.[11]

Previous scholarship has focused largely on facial recognition technology and biometric authentication;[12] this Comment suggests that the increasing use of biometric technology in society will have an impact beyond the use of facial recognition technology. Specifically,

---

[5] *See* Gomes, *supra* note 1.

[6] Vivek Lakshman, *The Future of Biometric Authentication Lies Beyond Mobile Apps*, BIOMETRICUPDATE.COM (Dec. 23, 2018, 4:33 PM), https://www.biometricupdate.com/201812/the-future-of-biometric-authentication-lies-beyond-mobile-apps.

[7] *Id.*

[8] Sterling Miller, *The Basics, Usage, and Privacy Concerns of Biometric Data*, THOMSON REUTERS (July 20, 2022), https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data.

[9] Andrew Zarkowsky, *Biometrics: An Evolving Industry with Unique Risks*, SDTIMES (July 27, 2021), https://sdtimes.com/ai/biometrics-an-evolving-industry-with-unique-risks.

[10] *Id.*

[11] Hayley Tsukayama, *Trends in Biometric Information Regulation in the USA*, ADA LOVELACE INST. (July 5, 2022), https://www.adalovelaceinstitute.org/blog/biometrics-regulation-usa.

[12] *See, e.g.*, Yana Welinder, *Facing Real-Time Identification in Mobile Apps & Wearable Computers*, 30 SANTA CLARA HIGH TECH. L.J. 89, 89, 109 (2013).

this Comment argues that companies use biometric data outside of its intended purpose—for security and authentication purposes—and the ease in which this data is collected has increased with the invention of mobile apps. Furthermore, the complicated landscape surrounding data privacy—specifically biometric data—has made it challenging for private companies to stay compliant with both federal and state law.[13] And more importantly, the lack of transparency surrounding the collection of sensitive data has eroded consumer trust and control.[14]

Part II of this Comment outlines the use of biometric data as technology has advanced and weighs the advantages and disadvantages of biometric data collection. Part III explores current privacy regulations overseeing mobile apps' collection and use of biometric data and assesses the general privacy issues surrounding them. Part III also details the current state of biometric privacy in the United States and the European Union, and highlights considerations for a federal biometric privacy law. Part IV examines the implications of a biometric-specific federal privacy law versus a comprehensive federal privacy law, and offers support for enacting a comprehensive US privacy law. Part V briefly concludes.

II. COMPETING INTERESTS OVER BIOMETRIC DATA USE

Part II discusses how biometrics have advanced alongside technology and evaluate how various industries have used biometrics. Furthermore, this Part discusses privacy concerns that have arisen as biometric technology has advanced.

A. *Background on Biometrics*

The use of biometrics is rooted in the principle of human identification and recognition. Characteristics of people's faces are used to define and recognize them daily and subconsciously. The classification of fingerprints as an identification method began in the late 1800s, and the concept of eye pattern identification arose in the

---

[13] *See* Eliza Simons, Note, *Putting a Finger on Biometric Privacy Laws: How Congress Can Stitch Together the Patchwork of Biometric Privacy Laws in the United States*, 86 BROOK. L. REV. 1097, 1101 (2021) (explaining that the various state laws regarding biometric privacy have created an inefficient and complicated landscape).

[14] *See, e.g.*, Lisa Joy Rosner, *How Biometric Data Will Shift the Privacy Conversation*, FORBES (July 2, 2019, 8:30 AM), https://www.forbes.com/sites/forbescommunicationscouncil/2019/07/02/how-biometric-data-will-shift-the-privacy-conversation (discussing how transparency and trust are critical factors impacting whether consumers would share their data with companies).

1900s.[15] The historical timeframe of biometrics suggests that biometric technology has been developing for hundreds of years, so it should not come as a surprise that, in the age of technology, individuals are now able to unlock their front door with a fingerprint.[16] What is troublesome, however, is the ways in which people have become numb to the sharing of their most personal and sensitive data, and in doing so, how individuals may have lost a sense of control over basic human characteristics. The following section discusses how government actors, the health care industry, and private companies have used biometric technology in the United States for security and authentication purposes.

Biometric data has many uses for government organizations, private companies, employers, and the health care industry. The unchanging nature of biometrics creates an appeal for private companies, businesses, and the government to use the data for identification and tracking.[17] Biometric data is increasingly used in the workplace as a means of more secure access control to private areas, building entry, and access to shared devices, like coffee machines and printers.[18] As a result of the COVID-19 pandemic and work from home procedures, more employers have utilized biometric authentication to create a more secure method of logging on from home.[19] The government also uses biometrics. For example, the Department of Homeland Security uses biometrics for "detecting and preventing illegal entry into the United States, granting and administering proper immigration benefits, vetting and credentialing, facilitating legitimate

---

[15] *See* Stephen Mayhew, *History of Biometrics*, BIOMETRICUPDATE.COM (Feb. 1, 2018, 11:43 AM), https://www.biometricupdate.com/201802/history-of-biometrics-2 (discussing the timeline of biometric technology development beginning with the first capture of hand images in 1858 to the use of fingerprint scanners on smartphones in 2013).

[16] *See id.*

[17] *See* Anna L. Metzger, Comment, *The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy*, 50 LOY. U. CHI. L.J. 1051, 1053 (2019); *see also* Simons, *supra* note 13, at 1098 (discussing how the distinctive nature of biometric data provides a secure and convenient means of identification and authentication for private companies).

[18] Drew Robb, *The Future of Biometrics in the Workplace*, SHRM (Feb. 22, 2022), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/the-future-biometrics-workplace.aspx.

[19] *See id.*

travel and trade, enforcing federal laws, and enabling verification for visa applications to the [United States]."[20]

The health care industry uses biometrics for both patient identification and authentication. Linking patients to their medical records and history creates a more accurate and efficient system in health care.[21] For example, health care providers and administrators have begun utilizing biometrics as a means of checking individuals into appointments at health care facilities.[22] This technology has helped in "decreasing wait time, reducing staffing needs, and protecting patient privacy by preventing patients from having to divulge personal health information during the check-in process."[23]

As technology advances, actors both in and out of the health care industry utilize mobile health apps (mHealth apps), which track diet and exercise, sleep patterns, and manage stress and anxiety to assist individuals in navigating their own health.[24] mHealth apps have potential benefits for individual health. As more people are able to take charge of their health, individuals may be able to better monitor illness and disease, and preventative care may improve.[25] For example, diabetes management apps assist people in tracking glucose levels and calculating insulin doses.[26] Many physicians promote mHealth apps for creating health management and intervention solutions because the apps provide more efficient access and communication options for patients.[27] Biometrics has played an important role in the advancement of technology within the health care space; still, individuals may be rightfully concerned over how companies may misuse their personal data on apps.

---

[20] *Biometrics*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/biometrics (May 5, 2023).

[21] Bill Siwicki, *Biometrics Entering a New Era in Healthcare*, HEALTHCARE IT NEWS (July 30, 2018, 9:19 AM), https://www.healthcareitnews.com/news/biometrics-entering-new-era-healthcare.

[22] Jordan T. Shewmaker, Note, *New Frontiers in Medical Privacy: Protecting the Biometric Data of Patients in the Healthcare Industry*, 106 KY. L.J. 813, 818 (2018).

[23] *Id.* at 818–19.

[24] *See How Mobile Apps Are Improving Healthcare: Saving Costs, Saving Lives*, MINDSEA, https://mindsea.com/health-apps (last visited Oct. 15, 2023).

[25] *See id.*

[26] Anuja Vaidya, *Key Features of mHealth Apps & Trends in Use*, MHEALTH INTEL. (May 13, 2022), https://mhealthintelligence.com/features/key-features-of-mhealth-apps-trends-in-use.

[27] Jamie Lynn Flaherty, Comment, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 419 (2014).

B. *Privacy Concerns over Biometrics*

Biometric data can potentially create more secure work environments and protect individual privacy on a broader scale, as described above. But biometric data is not without its issues. When private companies utilize data from consumers, there is always a risk of a data breach. A biometric data breach, however, presents different risks than other data breaches. For example, when hackers gain access to biometric data and identifiers such as fingerprints, retinal and facial scans, or voiceprints, they gain information that remains linked to the individual forever. Hackers can use stolen biometric information to access information connected to the individual, like banking information and digital wallets, which can ultimately lead to identity theft.[28]

Further concern over the use of biometric data involves its accuracy in application, which has presented both privacy and equity issues. Studies have revealed the bias apparent in algorithms used in facial recognition technology, which may be due to the fact that Black individuals are less likely to be included in the data sets used within algorithms for facial recognition technology.[29] As a result, biometric technology has often misidentified more Black people than White people, and this trend is expected to continue unless adequately addressed.[30] There have also been reported inequalities regarding the success of facial recognition technology amongst men and women, though researchers have not yet come up with valid reasoning behind these inequalities.[31] While this issue often emerges in the context of police investigations, it highlights the fact that there are limitations to biometric technology as it is used today.

Subsection 1 discusses privacy concerns regarding biometric use as a result of the COVID-19 pandemic and recent political movements

---

[28] Ryan Toohil, *Fingerprint Identity Theft: How to Keep Your Devices Secure*, AURA (July 26, 2023), https://www.aura.com/learn/fingerprint-identity-theft.

[29] *See* Tsukayama, *supra* note 11.

[30] *See, e.g.*, *id.* ("The use of facial recognition has led to the wrongful arrests of at least three Black men . . . . All of them could provide clear evidence that they were in different places at the time of the crimes they were arrested for . . . . Yet all three men were charged based on 'evidence' from facial recognition software.").

[31] *See* Jim Nash, *Facial Recognition Researchers Look for a Culprit in Gender Inequality, Come Up Empty*, BIOMETRICUPDATE.COM (Feb. 26, 2020, 2:48 PM), https://www.biometricupdate.com/202002/facial-recognition-researchers-look-for-a-culprit-in-gender-inequality-come-up-empty.

surrounding abortion. Subsection 2 explains general privacy concerns that have emerged over the use of data collection on mobile apps.

1. Biometrics and Tracking

The use of biometrics has given rise to specific concerns surrounding tracking. As discussed below, these concerns have heightened in the past few years, following the COVID-19 pandemic, and even more recently, after the Supreme Court's *Dobbs v. Jackson Women's Health Organization* decision that struck down the constitutional right to an abortion.[32] Following *Dobbs*, there has been increased concern over the ways in which private companies collect sensitive health information without proper privacy protections in place. Most notably, concern has increased over law enforcement's ability to access the data that these companies collect.[33]

Collection of location and biometric data is how people are tracked, and the *Dobbs* decision has raised questions over how companies not covered by existing privacy laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), use biometric data without individuals' consent.[34] Privacy experts are concerned that—without a federal privacy law in place—state officials could track those seeking abortion care through their digital footprint.[35] In June 2022, as a response to these concerns, Senators Ron Wyden and Mazie Hirono and Representative Sara Jacobs introduced the My Data, My Body Act to protect personal reproductive health data collected by mobile apps and websites.[36] If enacted, the act would limit the collection and storage of data to only what is necessary for the success of the product.[37] Similarly, advocates have called for a comprehensive federal privacy law that would protect against reproductive privacy in the wake of *Dobbs*.[38] Though reproductive

---

[32] *See* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2228 (2022).

[33] *See* Allison Grande, *Top Privacy Developments of 2022: Midyear Report*, LAW360 (July 22, 2022, 9:14 PM), https://www.law360.com/articles/1513282/top-privacy-developments-of-2022-midyear-report.

[34] *Id.*

[35] *Id.*

[36] Allison Grande, *Dems Call for FTC Probe of Mobile Tracking by Apple, Google*, LAW360 (June 24, 2022, 9:53 PM), https://www.law360.com/articles/1506062.

[37] *Id.*

[38] *See* Cameron F. Kerry, *How Comprehensive Privacy Legislation Can Guard Reproductive Privacy*, BROOKINGS (July 7, 2022), https://www.brookings.edu/blog/techtank/2022/07/07/how-comprehensive-privacy-legislation-can-guard-reproductive-privacy (discussing the potential for state

privacy is beyond the scope of this Comment, this issue highlights a recent movement among consumers and privacy experts to initiate a comprehensive privacy law that would protect consumers against the collection of all data.

Most notably, contact tracing apps emerged during the COVID-19 pandemic as a means of controlling and combatting the spread of disease.[39] These apps collect and record an individual's personal data and health information when an individual becomes infected with the virus.[40] Many of the apps utilize biometric data in order to keep user data secure.[41] The purpose is to monitor app users' infection and keep track of contact among users to minimize exposure.[42] These apps provide a good example of how the government uses biometric data collection and evaluation of user health data to advance public health goals. Yet, contract tracing apps have also raised concerns regarding the dangers of using biometric data outside of its intended scope—beyond the realm of many users' understanding. In the United States, many states hesitated to initiate biometric surveillance in the face of privacy concerns yet had considered the use of contact tracing apps and vaccine passports with facial recognition technology to monitor disease; these apps, however, were voluntary and permitted users to opt into data collection.[43]

Privacy concerns have emerged internationally, specifically in South Korea, Singapore, Australia, and Poland.[44] In South Korea, following its "COVID-19 success story" with the assistance of vigorous

---

prosecutors to seek evidence from mobile apps regarding a woman's digital tracks as they relate to menstrual cycles, abortions, and communications with health care providers).

[39] Jami Vibbert & Nancy L. Perkins, *COVID-19 Contact-Tracing Apps: What Privacy Law Will Apply?*, ARNOLD & PORTER: ADVISORIES (June 10, 2020), https://www.arnoldporter.com/en/perspectives/advisories/2020/06/covid-contact-tracing-apps-what-privacy.

[40] *Id.*

[41] *Id.*; *see also* Gomes, *supra* note 1.

[42] *See* Vibbert & Perkins, *supra* note 39.

[43] *See* Jianchen Liu, *Privacy Risks in Using Facial Recognition for Contact Tracing*, COLUM. J. TRANSNAT'L L. (Mar. 13, 2021), https://www.jtl.columbia.edu/bulletin-blog/privacy-risks-in-using-facial-recognition-for-contact-tracing.

[44] *See, e.g.*, Umberto Bacchi, *Pandemic Surveillance: Is Tracing Tech Here to Stay?*, THOMSON REUTERS (Mar. 9, 2022), https://news.trust.org/item/20220304092506-aky0c; Brianna Navarre, *COVID-19 Data-Driven Spark Privacy and Abuse Fears*, U.S. NEWS (Jan. 19, 2022, 6:00 AM), https://www.usnews.com/news/best-countries/articles/2022-01-19/contact-tracing-biometrics-raise-privacy-concerns-amid-pandemic.

testing and tracing, the government announced its planned use of artificial intelligence (AI), facial recognition technology, and closed-circuit television (CCTV) technology to track infections among people.[45] This plan spiked privacy concerns, as many individuals have questioned whether these surveillance practices will persist beyond their necessary use post-pandemic.[46]

Furthermore, Singapore announced that police may use any data collected through its contact tracing app in criminal investigations, while Australia has authorized the utilization of facial recognition technology in identifying whether people stayed at home throughout quarantine.[47] Poland's home quarantine app uses geolocation and facial recognition to permit authorities to keep track of compliance with isolation requirements.[48] While many individuals may feel safer through contact tracing apps and other means of public health surveillance, others fear that they are "being spied on" and have pushed for the phasing out of these apps.[49]

Many specialists are concerned that biometric technology's current use has allowed for a sense of normalcy regarding surveillance technology, even though governments used it prior to the pandemic.[50] For example, Spain adopted the use of facial recognition technologies in casinos and bus stops in the past year, which is clearly outside of public health uses.[51] In the United States, biometric information collected and stored through contact tracing apps, when associated with health information, may be covered under HIPAA—depending on who uses the system and whether they are a covered entity or business associate.[52] Society can learn from contact tracing apps that the collection of biometric data through surveillance is just one of the ways individuals become numb to the way that third parties use their

---

[45] Bacchi, *supra* note 44.

[46] *Id.*

[47] *Id.*

[48] Navarre, *supra* note 44.

[49] Frank Hersey, *Can the World Shake Off COVID-19 Biometric Surveillance?*, BIOMETRICUPDATE.COM (Mar. 11, 2022, 2:38 PM), https://www.biometricupdate.com/202203/can-the-world-shake-off-covid-19-biometric-surveillance.

[50] *See* Navarre, *supra* note 44; *see also infra* notes 71–77 and accompanying text.

[51] *Id.*

[52] Divya Ramjee et al., *COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance*, 2021 CARDOZO L. REV. DE NOVO 101, 132 (2021), https://doi.org/10.2139/ssrn.3733071.

data. Of course, contact tracing apps provided an immense benefit to society during the pandemic as a means of controlling and maintaining the virus.[53] But many users failed to see how private entities collected their biometric information and how it would eventually be used by third-party organizations and the government.

2. General Privacy Concerns Regarding Mobile Apps

Mobile apps have raised general privacy concerns as technology has advanced. Recently, lawmakers urged the "[Federal Trade Commission (FTC) to] investigate Apple['s] and Google's role in transforming online advertising into an intense system of surveillance that incentivizes and facilitates the unrestrained collection and constant sale of Americans' personal data."[54] Following this letter from lawmakers, as well as the Court's ruling in *Dobbs*, the FTC announced that it would be investigating and "cracking down" on the illegal sharing of sensitive personal data.[55] Both Apple and Google permit users to "opt-out" of this tracking;[56] however, lawmakers insist that the lack of transparency between the tech giants and users has exposed Americans to serious privacy harms.[57] It has become well-known that apps sell data to companies like Facebook for the purpose of targeted marketing.[58] In fact, selling data for the purpose of targeted marketing has become a primary component of how apps and private companies utilize such data.[59] For example, patents by Meta, Facebook's parent

---

[53] *See* Dyani Lewis, *Contact-Tracing Apps Help Reduce COVID Infections, Data Suggest*, NATURE: NEWS, https://www.nature.com/articles/d41586-021-00451-y (Feb. 26, 2021) (discussing the results of multiple studies that found that contact tracing apps in England and Wales prevented COVID infections by notifying the contacts of individuals who reported positive COVID results).

[54] *See* Grande, *supra* note 33.

[55] Bonnie Eslinger, *After Dobbs, FTC Pledges to Police Sharing of Sensitive Data*, LAW360 (July 11, 2022, 9:53 PM), https://www.law360.com/articles/1510555.

[56] *See* Nico Grant, *Google to Let Android Users Opt Out of Tracking, Following Apple*, BLOOMBERG (June 3, 2021, 3:50 PM), https://www.bloomberg.com/news/articles/2021-06-03/google-to-let-android-users-opt-out-of-tracking-following-apple#xj4y7vzkg.

[57] *See* Eslinger, *supra* note 55.

[58] *See* Alessandro Mascellino, *Meta Patents Suggest Biometric Data Capture for Personalized Advertising*, BIOMETRICUPDATE.COM (Jan. 24, 2022, 11:20 AM), https://www.biometricupdate.com/202201/meta-patents-suggest-biometric-data-capture-for-personalized-advertising.

[59] *See, e.g.*, *id.*

company, revealed possible plans to capture users' biometric data in order to provide "hyper-targeted advertising and sponsored content."[60]

In 2014, the FTC directed an investigation that found that free mHealth apps collectively sent personal data and information to seventy-six various third-party organizations.[61] Specific examples of the data collected from these apps included "device information; consumer-specific identifiers; unique device IDs capable of allowing third parties to track users' devices across apps; unique third-party IDs capable of allowing third parties to track users' devices across apps; and consumer information such as exercise routine, dietary habits, and symptom searches."[62] The above-mentioned study pertains to fitness apps; the concern over privacy, however, extends to all mHealth apps that collect other personal data, like biometric data.[63] When used in this way, consumers' personal data could be linked to these biometric identifiers and has the potential to put their privacy in jeopardy.

Critics have accused mHealth apps of sharing user concerns and searches that have the potential to be linked to other identifying information. In fact, privacy concerns surrounding mHealth apps are rooted in the fact that "[b]ig data collectors such as brokers or ad companies" can collect user identifiers and may ultimately "piece together someone's behavior or concerns using multiple pieces of information or identifiers."[64] Though these concerns do not explicitly address the collection of biometric data and mostly focus on privacy surrounding users' health concerns, it raises the question of how apps may eventually link this personally identifying information to other personal data, such as facial scans and fingerprints.

---

[60] *Id.*

[61] Alexis Guadarrama, Comment, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 HOUS. L. REV. 999, 1013 (2018).

[62] *Id.* (quoting FED. TRADE COMM'N, SPRING PRIVACY SERIES: CONSUMER GENERATED AND CONTROLLED HEALTH DATA 10 (2014)).

[63] *Id.*

[64] Tatum Hunter & Jeremy B. Merrill, *Health Apps Share Your Concerns With Advertisers. HIPAA Can't Stop It.*, WASH. POST, https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy (Sept. 22, 2022, 10:26 AM).

III. LEGAL PROTECTIONS OF BIOMETRIC DATA

Currently, the United States lacks a comprehensive federal privacy law, yet alone a federal biometric-specific privacy law. The absence of an all-encompassing federal privacy law results in a difficult privacy landscape to navigate, for both consumers and private businesses. Following the discussion in Part II, which outlined the usage of biometric data through mobile apps, Section A discusses the current federal oversight of biometric data, and Section B reviews the various jurisdictions with biometric privacy laws in place and evaluates how each law has contributed to the biometric privacy legal framework. Section A and Section B also explain how critics have scrutinized mobile apps for lack of data privacy protections and evaluate how federal oversight for biometric privacy has contributed to that scrutiny. Section C analyzes how biometric privacy regulations and data privacy laws have developed internationally. Finally, Section D discusses legislation that states have proposed in response to growing concerns over biometric privacy.

A. *Biometric Privacy Under General Federal Privacy Protections*

There are several federal statutes and agencies that aim to protect against the collection of consumer data in the face of an increasingly technological society. The HIPAA Privacy Rule protects patient health information in certain health care settings.[65] The Children's Online Privacy Protection Act (COPPA) protects children's personal information and data on online platforms.[66] And regulatory agencies like the FTC play a role in the enforcement and investigation of data misuse.[67] Put together, the United States takes a fragmented approach to data privacy, specifically biometric privacy, leaving open many holes where consumer data goes largely unprotected. This Part assesses the federal regulations and agencies that currently oversee biometric privacy. Using mobile apps as an example, this Part also analyzes how gaps are left open by this federal oversight.

---

[65] *See Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. [hereinafter *HIPAA Privacy Rule*], https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (Oct. 19, 2022).

[66] *See Children's Online Privacy Protection Rule ("COPPA")*, FED. TRADE COMM'N, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (last visited Dec. 18, 2023).

[67] *See* Guadarrama, *supra* note 61, at 1010–11.

1. Biometric Data as Protected Under HIPAA

The HIPAA Privacy Rule (Privacy Rule), which the government promulgated pursuant to HIPAA and in response to privacy concerns, set guidelines for the protection of specified health information in order to address the "use and disclosure of individuals' health information," known as "protected health information" (PHI).[68] The Privacy Rule protects health information while simultaneously supporting the collection of health information necessary to promote the quality of health care.[69] The Privacy Rule includes biometric data under the category of individually identifiable health information, which is defined as "biometric identifiers, including finger and voice prints."[70]

HIPAA applies to covered entities, and in some circumstances, their business associates.[71] Covered entities include health care providers, health plans, and health care clearinghouses.[72] The Privacy Rule defines a business associate as "a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information."[73] When a business associate acts with a covered entity to conduct health care functions, there must be a written business associate contract between the parties that establishes the responsibilities of the business associate; these contracts require compliance with HIPAA rules.[74] Therefore, HIPAA will only cover mHealth apps when the organization behind the app operates as a covered entity, or when the organization works for a covered entity and they utilize a business associate agreement.[75] Typically, mHealth app companies qualify as a business associate of a covered entity when the company "creat[es] or offer[s] the app on behalf of a covered entity,"

---

[68] *See HIPAA Privacy Rule*, *supra* note 65.

[69] *Id.*

[70] *Id.*

[71] *See Covered Entities and Business Associates*, U.S DEP'T HEALTH & HUM. SERVS. (June 16, 2017) [hereinafter *Covered Entities and Business Associates*], https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[72] *Id.*

[73] *HIPAA Privacy Rule*, *supra* note 65.

[74] *Id.*

[75] *Id.*

in which case it is required to comply with HIPAA.[76] For example, when a consumer uses a mHealth app to monitor her glucose levels and blood pressure using readings that she obtained herself with home equipment, she simply uses the mHealth app as a consumer without involving her health care providers; therefore, HIPAA will not protect any information that the app collects.[77]

As an example of the ways in which the regulatory framework surrounding data collection may confuse or mislead consumers, women's mHealth app, Ovia Health ("Ovia"), reported that some of the health data collected through the app may be subject to HIPAA regulations, but not all of the data.[78] Ovia's privacy policy states that data is covered under HIPAA "if a person receives the app as a benefit from their health plan or health care provider."[79] Therefore, if the consumer uses the free version of the app as a consumer, rather than using the app through their health insurer or employer health plan, HIPAA will not apply.[80] Unfortunately, consumers not well-versed in the language of HIPAA may not understand this.

Important in the context of biometric data and privacy, HIPAA contains a breach notification rule, which "requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information."[81] A breach occurs when there is prohibited use of data under the Privacy Rule that endangers the security of PHI, which includes biometric data.[82] Covered entities must notify the impacted individuals, the secretary of the Department of Health and Human Services (HHS), and on occasion, the media.[83] The HIPAA breach notification rule provides an example of an additional requirement for companies using PHI—

---

[76] U.S DEP'T HEALTH & HUM. SERVS., HEALTH APP USE SCENARIOS & HIPAA 1 (2016), https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.

[77] *See id.* at 2.

[78] Erin Jones, *No, Health Data from Most Period-Tracking Apps Is Not Protected Under HIPAA*, VERIFY: HEALTH, https://www.verifythis.com/article/news/verify/health-verify/period-tracking-apps-hipaa-privacy-rules-law-fact-check/536-bf44e08c-cc5f-4ee8-997a-c15e0060081a (June 24, 2022, 2:26 PM).

[79] *Id.*

[80] *Id.*

[81] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (July 26, 2013).

[82] *Id.*

[83] *Id.*

a requirement that should, in theory, hold companies accountable when they are collecting and storing personal data by encouraging them to use caution to avoid a breach.

2. Coverage by Other Federal Agencies and Regulations

Private companies that collect personal data through mHealth apps but are outside the scope of the regulatory framework set up by HIPAA, are left in a largely unregulated field.[84] Other agencies involved in the indirect regulation of data collection by mobile apps include the FTC, which investigates companies accused of making misleading claims about privacy and security, especially where injury to the consumer is likely.[85] Agencies within the Office of Civil Rights (OCR), the HHS, and the Food and Drug Administration (FDA) all have the ability to regulate the health information transmitted by mHealth apps, but their authority is limited in scope and generally does not apply to the apps not covered under HIPAA.[86] Therefore, for mHealth apps, many companies find themselves "navigating the segmented regulatory framework."[87]

Third-party mHealth apps may fall under the purview of section 5(a) of the Federal Trade Commission Act (FTCA), "which forbids unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce."[88] The FTC also contains a health breach notification rule, which "requires vendors of personal health records that contain individually identifiable health information

---

[84] *See* Guadarrama, *supra* note 61, at 1010 (discussing how apps that are outside of the covered entity category are left to the discretion of agencies that do not typically regulate electronic health information).

[85] *Id.* at 1011.

[86] *Id.* at 1011–12. "The Office of Civil Rights . . . enforces the HIPAA Rules" and the HIPAA Privacy Rule, and the FDA's enforcement only regulates apps that are subject to FDA medical device regulations; therefore, many mHealth apps "fall outside of the FDA's purview because they do not qualify as medical devices." *Id.* at 1011–12.

[87] Chad Ehrenkranz et al., *Digital Health Cos. Should Expect More Scrutiny Amid Growth*, LAW360 (Aug. 16, 2022, 6:44 PM), https://www.law360.com/articles/1521440/digital-health-cos-should-expect-more-scrutiny-amid-growth. mHealth apps are regulated by three main "pillars": HIPAA, the Federal Food, Drug and Cosmetic Act (FDCA), and the FTC. *Id.* HIPAA and the FDCA are more limited in the mHealth apps that they cover, while the FTC attempts to fill this gap. *Id.* The FDA enforces the FDCA, and the agency "focuses its regulatory oversight on a small subset of mHealth apps that may affect the performance or functionality of regulated medical devices . . . ." *Id.* The FTC oversees the regulatory gap through enforcement of section 5(a). *Id.*

[88] *Id.*; *see also* 15 U.S.C. § 45(a).

created or received by health care providers, and personal health record-related entities to notify US consumers, the FTC and, in some cases, the media, if there is a breach of unsecured identifiable health information."[89] An example of a mHealth app that came under the FTC's scrutiny is Flo Health ("Flo").[90] The FTC investigated Flo, a women's mHealth app, in January 2021 when it alleged that Flo shared personal data collected via the app with companies such as Google and Facebook for marketing and advertising purposes.[91] The FTC later settled the issue with Flo but required that Flo obtain consent from its users before sharing personal data with third parties.[92]

Also in January 2021, the FTC signaled its renewed interest in the collection of biometric data, specifically facial scans, through its settlement with Everalbum, Inc. ("Everalbum"), the developer of a photo storage app known as Ever.[93] This settlement signified the FTC's first enforcement action that specifically focused on facial recognition technology.[94] The FTC's complaint alleged that Everalbum violated section 5 of the FTCA by engaging in deceptive acts or practices when the app retained users' images after promising to delete them.[95] The settlement required "that Everalbum delete any models and algorithms based on any biometric information collected from users of the Ever app."[96]

The investigation of Everalbum also depicts how the complicated legal landscape surrounding biometric privacy works in application. For example, Ever users living "in Texas, Illinois, Washington, and the European Union"—all jurisdictions with biometric privacy laws in place—were able to opt into, or out of, the use of facial recognition technology on the app.[97] Meanwhile, users not within those jurisdictions "were not given the opportunity to opt in to the use of facial recognition technology—rather, the technology was enabled by default—and they were not able to turn the technology on and off."[98]

---

89 *Id.* (footnotes omitted).

90 *See* Jones, *supra* note 78.

91 *Id.*

92 *Id.*

93 *See* Janis Kestenbaum et al., *FTC Deal with Photo App May Signal More Biometric Scrutiny*, LAW360 (Feb. 2, 2021), https://www.law360.com/articles/1350111.

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.*

Thus, a major problem in this regulatory gray area is that consumers are generally not aware of the fact that privacy policies differ between states, and they do not have the same protection as other consumers do.

This issue also appears with mHealth apps, when users fail to realize that HIPAA does not apply to the mHealth apps that they use, and that the app may use collected health data in a way that is outside the scope of their understanding.[99] Linda Malek, chair of the firm Moses & Singer's Healthcare Privacy and Cybersecurity group, argued that what is needed is a "comprehensive regulation or legislation that imposes consistent guidance across various players within the industry that may have access to health data."[100]

In the health care context, some mHealth apps appear on the surface to fall under the purview of HIPAA, yet are not actually regulated under the federal statute. For example, Fitbit, a leader in wearable fitness technology, is not a covered entity under HIPAA because it collects users' health data for their own use, rather than working in conjunction with a covered entity, such as a physician or other health care provider.[101] Therefore, even though it is collecting information that would seemingly fall under the personal health information category of the Privacy Rule, such as an individual's height, weight, and heart rate, HIPAA will not apply, leaving users no choice but to place their sole trust in the company's privacy policy.[102]

A 2021 study about the privacy practices of mobile apps suggests that users are not properly informed about the reality of the risks related to their usage.[103] Meanwhile, mHealth apps account for a large portion of the apps on both Google Play and the Apple Store.[104] A

---

[99] *See* Jill McKeon, *The Quest to Improve Security, Privacy of Third-Party Health Apps*, HEALTH IT SEC. (Apr. 12, 2022), https://healthitsecurity.com/features/the-quest-to-improve-security-privacy-of-third-party-health-apps.

[100] *Id.*

[101] *See* Ted North, *Google, Fitbit, and the Sale of Our Private Health Data*, HEALTH L. & POL'Y BRIEF: BLOG (Nov. 18, 2019), https://www.healthlawpolicy.org/2019/11/18/google-fitbit-and-the-sale-of-our-private-health-data.

[102] *Id.*

[103] *See Study Finds "Serious Problems with Privacy" in Mobile Health Apps*, BMJ (June 16, 2021), https://www.bmj.com/company/newsroom/study-finds-serious-problems-with-privacy-in-mobile-health-apps.

[104] *See id.* ("Of the 2.8 million apps on Google Play and the 1.96 million apps on Apple Store, an estimated 99,366 belong to medical and health and fitness categories . . . .").

study conducted at Macquarie University in Australia compared the privacy policies of over fifteen thousand free mHealth apps with that of eight thousand non-mHealth apps and found that "while mHealth apps collected less user data than other types of mobile apps, 88 [percent] could access and potentially share personal data."[105] Furthermore, about 28 percent of the mHealth apps did not provide a privacy policy, and about 25 percent participated in user data transmissions that violated what they stated in their privacy policy.[106] These statistics highlight the lack of transparency between private companies and consumers and suggest the urgent need for a federal privacy law that will keep companies in check and protect consumer data. Additionally, without a bright line rule for compliance with biometric data use, it is up to individual companies to ensure data privacy, and up to consumers themselves to be mindful of where they put their data.

B. *US States with Biometric Privacy Laws*

State legislatures, in the absence of a federal measure, have begun cracking down on private companies' collection and use of biometric data.[107] Illinois led the trend in 2008 with the introduction of the Biometric Information Privacy Act (BIPA).[108] BIPA is the most comprehensive state biometric-specific privacy law to date.[109] Other states, like Washington and Texas, followed suit in enacting biometric-specific privacy laws.[110] The Illinois law is considered a leader among the other states.[111] As of 2023, eleven states—Nevada, Kentucky, Maine, Maryland, Missouri, Arizona, Vermont, Minnesota, Mississippi, Tennessee, and New York—have proposed, but not yet passed,

---

105 *Id.*

106 *Id.*

107 *See* Molly S. DiRago et al., *A Fresh "Face" of Privacy: 2022 Biometric Laws*, TROUTMAN PEPPER: ARTICLES + PUBLICATIONS (Apr. 5, 2022), https://www.troutman.com/insights/a-fresh-face-of-privacy-2022-biometric-laws.html.

108 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.

109 *See id.*

110 *Id.*

111 *Id.*

biometric-specific privacy bills; one state—Massachusetts—is actively legislating a biometric-specific law.[112]

Privacy experts suggest that companies collecting and using biometric data remain vigilant of state biometrics bills should they become laws that require compliance.[113] Much of the difficulty that arises from the patchwork of state laws regarding biometric privacy stems from their inconsistency, which makes it hard for a company to keep track of compliance under each statute. For example, the definition of a "biometric identifier" changes from Illinois, to Washington, and so on.[114] Not only do the laws differ in the definition of biometric data but they also differ in application, enforcement, and relief awarded, making it exceedingly difficult for both consumers and private companies to keep up. Subsection 1 discusses the Illinois statute protecting biometric privacy and the subsequent legal ramifications that have followed this statute. Subsection 2 explains and analyzes both the Texas and Washington statutes protecting consumers' biometric data.

1. Illinois: Biometric Information Privacy Act

BIPA has received significant attention within the US biometric privacy landscape—and it has also proved the most stringent.[115] In enacting BIPA, the Illinois state legislature acknowledged that biometric data presents a unique risk to privacy issues, specifically stating that biometrics "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."[116]

Under BIPA, biometric information includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[117] Interestingly, BIPA goes to great lengths to state what is not considered a biometric identifier, such as writing samples, demographic data,

---

[112] *See Tracking U.S. State Biometric Privacy Legislation*, HUSCH BLACKWELL, https://www.huschblackwell.com/2023-state-biometric-privacy-law-tracker (June 20, 2023).

[113] *See* DiRago et al., *supra* note 107.

[114] *See, e.g.*, 740 ILL. COMP. STAT. 14/10 (2023); WASH. REV. CODE § 19.375.010 (2023).

[115] *See* Prescott, *supra* note 108.

[116] 740 ILL. COMP. STAT. 14/5 (2023).

[117] 740 ILL. COMP. STAT. 14/10 (2023).

donated organs, X-rays, photographs, and many more categories.[118] BIPA protects biometric data by requiring entities that collect, store, and use biometric identifiers, as defined above, to comply with requirements, such as obtaining informed consent from the consumer, creating a retention schedule for such data, and refraining from profiting from the sale of such data.[119]

Perhaps the most distinctive feature of BIPA, and the part that is both widely praised and criticized, is the private right of action. The statute states that "[a]ny person aggrieved by a violation of this [a]ct shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party."[120] An individual suing under BIPA may collect $1,000 in liquidated damages, or actual damages, depending on which is greater for each violation of the statute.[121] Furthermore, private entities that intentionally or recklessly violate BIPA could owe up to $5,000 in liquidated or actual damages per violation, and in some cases, reasonable attorneys' fees and injunctive relief may be awarded.[122] For big companies facing class action lawsuits and multiple violations, BIPA has the potential to result in hefty damages.[123] This Part discusses the litigation that has followed BIPA and analyzes arguments in support and against BIPA.

As previously explained, BIPA has garnered both support and criticism over its private right of action. Though BIPA took effect in 2008, it did not become widely known until 2015, when several lawsuits involving private companies, including Google and Shutterfly, were filed.[124] Google came under scrutiny in 2016 for allegedly using Google Photos to scan facial geometry of individuals without their consent—an explicit violation of BIPA.[125] The District Court for the Northern District of Illinois rejected Google's argument that facial geometric scans were not considered biometric identifiers under BIPA,

---

[118] *Id.*

[119] JACKSON LEWIS, ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT FAQS 2 (n.d.), https://www.jacksonlewis.com/sites/default/files/docs/IllinoisBIPAFAQs.pdf.

[120] 740 ILL. COMP. STAT. 14/20 (2023).

[121] *Id.*

[122] *Id.*

[123] *See* Emma Graham, Note, *Burdened by BIPA: Balancing Consumer Protection and the Economic Concerns of Businesses*, 2022 U. ILL. L. REV. 929, 938 (2022).

[124] *See* Metzger, *supra* note 17, at 1068 ("These cases [were] significant because they demonstrated that BIPA could hold companies domiciled outside of the state accountable for information collected in Illinois.").

[125] *See* Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1090 (N.D. Ill. 2017).

instead finding that Google was "using biology-based measurements to create a scan of facial geometry," which qualifies as a biometric identifier under the statute.[126] Though the court later dismissed the suit for the plaintiff's failure to show a concrete injury, this case is important because it broadened the statute's definition of biometric identifier.[127]

BIPA litigation has increased since then, partly due to the statute's broad private right of action, and partly due to the Supreme Court of Illinois' holding in the case of *Rosenbach v. Six Flags Entertainment Corp.*[128] Here, a minor alleged that the amusement park had violated BIPA by collecting his thumb print without his consent.[129] The Supreme Court of Illinois held that, to be considered an "aggrieved" party under BIPA, a plaintiff only needs to allege that there was a violation of BIPA, not that they experience an actual harm or injury.[130] The Ninth Circuit followed suit in *Patel v. Facebook, Inc.*, "suggest[ing] that challenges to Article III standing for future BIPA litigation in federal court lacked viability."[131] Following *Rosenbach*, Illinois courts were flooded with "hundreds of BIPA lawsuits."[132]

BIPA has also resulted in several class action settlements—many of which involve mobile apps. Recently, TikTok, the social media and video platform, began collecting individuals' biometric information, such as faceprints and voiceprints.[133] This led to a class action lawsuit in which claimants "alleged that TikTok violated BIPA by collecting

---

[126] *Id.* at 1095; Kelly Wong, *The Face-ID Revolution: The Balance Between Pro-Market and Pro-Consumer Biometric Privacy*, 20 J. HIGH TECH. L. 229, 249–50 (2020).

[127] Wong, *supra* note 126, at 250.

[128] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1200 (Ill. 2019).

[129] *See* Metzger, *supra* note 17, at 1076–77; *Rosenbach*, 129 N.E.3d at 1200–01.

[130] *Rosenbach*, 129 N.E.3d at 1206; Sojung Lee, Note, *Give Up Your Face, and a Leg to Stand on Too: Biometric Privacy Violations and Article III Standing*, 90 GEO. WASH. L. REV. 795, 808 (2022).

[131] Lee, *supra* note 130, at 809; *see also* Patel v. Facebook, Inc., 932 F.3d 1264, 1275 (9th Cir. 2019) (holding that a violation of a right established by BIPA was sufficient for a concrete injury).

[132] Lee, *supra* note 130, at 808.

[133] Sarah Perez, *TikTok Just Gave Itself Permission to Collect Biometric Data on US Users, Including 'Faceprints and Voiceprints,'* TECHCRUNCH (June 3, 2021, 6:57 PM), https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints. As of 2023, this case is currently pending in Illinois. Christopher Brown, *Suit Over At-Home Skin-Assessment Scans Advances Against J&J*, BLOOMBERG L. (Apr. 27, 2023, 12:55 PM), https://news.bloomberglaw.com/privacy-and-data-security/suit-over-at-home-skin-assessment-scans-advances-against-j-j.

users' faceprints without their consent."[134] The settlement, which resulted in a $92 million payment from TikTok, included forms of injunctive relief in which TikTok agreed to stop collecting consumers' biometric data unless done in accordance with applicable laws in Illinois.[135]

More recently, plaintiffs accused Johnson & Johnson (J&J) of violating BIPA by collecting and storing individuals' biometric data without their consent, an express violation of BIPA.[136] J&J's app, Neutrogena Skin360, collected individuals' facial scans in order to analyze the health of their skin and recommend skincare products based on the results of the scan.[137] Additionally, the data obtained from the facial scan was used to "improve the functionality of its artificial intelligence, or AI, assistant."[138] Neutrogena Skin360, however, failed to disclose the storage of this data and did not request a written release, a major requirement under BIPA.[139] Finally, the complaint alleged that the data collected from the facial scan was further linked to the user's generic personal and private information, including "sleep schedules, exercise routines, stress levels[,] and geographic location."[140]

Similarly, L'Oréal, a beauty company, created an online website that included a virtual try-on tool to test how products may look, while simultaneously scanning and collecting the individual's geometric facial data.[141] In doing so, L'Oréal allegedly violated several provisions of BIPA by failing to obtain informed consent from consumers prior to collecting facial scans; disclose how the consumers' biometrics obtained from the beauty tool would be used and retained; and provide a timeframe or specific purpose for which the data is

---

134 Hunton Andrews Kurth, *Judge Approves $92 Million TikTok Settlement*, THE NAT'L L. REV. (Aug. 9, 2022), https://www.natlawreview.com/article/judge-approves-92-million-tiktok-settlement.

135 *Id.*

136 Hayley Fowler, *J&J Unit Hit with BIPA Suit over Skin Care App's Face Scans*, LAW360 (May 26, 2022, 6:47 PM), https://www.law360.com/articles/1497471/j-j-unit-hit-with-bipa-suit-over-skin-care-app-s-face-scans.

137 *Id.*

138 *Id.*

139 *Id.*

140 *Id.*

141 Lauraann Wood, *L'Oréal Hit with Privacy Suit over Virtual Try-On Tool*, LAW360 (July 26, 2022, 4:18 PM), https://www.law360.com/articles/1515227/l-or-al-hit-with-privacy-suit-over-virtual-try-on-tool.

collected.[142] Though the privacy policy attempted to disclose the functions of its virtual try-on tool, it only referenced the photographs that users may upload or share with the company, and the policy did not reference how biometrics are used at all.[143]

These lawsuits provide examples of the ways in which biometric data may be used outside of the scope of the consumer's understanding. Similarly, these suits raise the concern that the absence of a comprehensive privacy law has resulted in an unregulated need of consumer data. Overall, the lawsuits highlight the lack of control consumers have over their personal information without a privacy law in place.

2. Texas and Washington Laws on Biometric Privacy

Texas was one of the first US States to enact a biometric-specific privacy law.[144] The state passed its law, known as the Capture or Use of Biometric Identifier Act (CUBI), in 2009, and it defines biometric identifiers as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[145] Unlike BIPA, the Texas statute does not create a private right of action, instead leaving it up to the Texas attorney general to bring the action and recover the civil penalty.[146] CUBI also requires notice and consent to the consumer prior to the capture of biometric data for a commercial purpose, and prohibits the sale and disclosure of biometric data, except for a few narrow circumstances.[147] Recently, the Texas attorney general filed a complaint against Meta, Facebook's parent company, alleging violations dating back to 2010 associated with the company's "face recognition" system.[148] The Texas attorney general has rarely enforced

---

142 *Id.*

143 *Id.* Plaintiffs filed a class action lawsuit against L'Oréal in May 2022, which is still pending. *Virtual 'Try-On' Technologies Face Mounting Legal Challenges*, PURDUE GLOB. L. SCH. (Aug. 7, 2023), https://www.purdueglobalawschool.edu/blog/news/virtual-try-on-technologies.

144 *See* DiRago et al., *supra* note 107.

145 TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2017); *see also* F. Mario Trujillo & Jon Frankel, *Texas Starts Enforcing Its Biometric Law*, ZWILLGENBLOG: PRIV., https://www.zwillgen.com/privacy/texas-cubi-law-and-biometric-privacy (June 13, 2023).

146 TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2017).

147 *See* Trujillo & Frankel, *supra* note 145 ("The law similarly bars the sale or disclosure of biometric identifiers, except in narrow circumstances like to complete an authorized financial transaction or for law enforcement purposes.").

148 *Id.*

this law, so the Meta litigation is expected to provide insight into how the law is applied, the substantive meaning of "biometric identifiers," and what is required for notice and consent.[149] The Texas attorney general also filed suit against Google, alleging that the company violated CUBI by failing to obtain Texans' consent prior to capturing facial scans and voice recordings.[150] The attorney general's recent approach toward biometric privacy enforcement reflects his desire to challenge "Big Tech."[151]

Washington is another state with a biometric privacy law in place. Under the law, biometric identifiers are defined as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[152] Notably, however, the Washington law does not include "a physical or digital photograph, video or audio recording[,] or data generated therefrom" under the definition of biometric identifiers, which differs from both Illinois and Texas by not including facial recognition data.[153] Washington's biometric privacy law is also enforceable under its Consumer Protection Act and does not contain a private right of action, unlike BIPA.[154] The law prohibits the enrollment of biometric data in any database for a commercial purpose without first providing notice and obtaining consent from the consumer and restricts the sale and disclosure of such data.[155] Again, this differs from both Illinois and Texas, who prohibit the activity of collecting and capturing biometric data, rather than enrolling the data.[156]

In an attempt to exercise even more control over the collection of biometric data, Washington state recently enacted the My Health, My Data Act ("MHMDA"), which seeks to provide consumers with even

---

149 *Id.*

150 Ali Sullivan, *Texas AG Accuses Google of Biometric Privacy Violations*, LAW360 (Oct. 20, 2022, 11:43 AM), https://www.law360.com/articles/1541813.

151 *Id.*

152 WASH. REV. CODE § 19.375.010 (2023).

153 *Id.*; *see also Washington Becomes the Third State with a Biometric Law*, INSIDE PRIV. (May 31, 2017), https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law ("[T]he statute will have limited application in the context of facial recognition technology.").

154 WASH. REV. CODE § 19.375.030 (2023).

155 *See Washington Becomes the Third State with a Biometric Law*, *supra* note 153.

156 *Id.*

more control over their personal health data.[157] Washington enacted the MHDMA in April 2023, providing two legal bases for processing a consumer's health-related data: consent or necessity.[158] The act includes "biometric data" as "information generated from an individual's physiological, biological[,] or behavioral characteristics that identifies a consumer, but is only covered *if it relates to health information*."[159] The definition of consumer is purposely broad and thus applies not only to Washington state residents but also to any individual whose consumer health data is collected in Washington.[160]

3. California's Consumer Privacy Act

California's Consumer Privacy Act (CCPA) was enacted in an effort to give users control over how their personal data is used and collected by private businesses.[161] The CCPA provides several rights to consumers, such as the right to know what data is being collected and how it is being used, and the right to opt out of the sale of their personal data, meaning that consumers can request that businesses stop the sale of any personal data collected.[162] The CCPA protects personal information, which includes biometric data, defined as "an individual's physiological, biological, or behavioral characteristics, including information pertaining to 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."[163] The CCPA also provides a non-exhaustive list of identifiers:

> [I]magery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.[164]

---

157 Amy Olivero & Anokhy Desai, *Washington's My Health, My Data Act*, IAPP, https://iapp.org/resources/article/washington-my-health-my-data-act-overview (Apr. 2023).

158 *Id.*

159 *Id.* (emphasis added).

160 *See id.*

161 *California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST.: OFF. OF THE ATT'Y GEN., https://oag.ca.gov/privacy/ccpa (May 10, 2023).

162 *See id.*

163 CAL. CIV. CODE § 1798.140(c) (West 2023).

164 *Id.*

The CCPA, however, is not confined to biometric data protection and therefore represents a state effort to protect biometric data "under a larger privacy umbrella."[165] As a comprehensive privacy law, the CCPA treats biometric data the same as all other personal data—meaning that there is no special or heightened protection provided for biometric data.[166] There is one exception to this, however; biometric data that is collected by a business from a user without that user's knowledge cannot be considered publicly available information.[167] This provision importantly recognizes the significance of consumer consent.

Following in the footsteps of BIPA, the CCPA provides a private right of action for California citizens to sue companies alleging that their personal data was misused.[168] And just like BIPA, this private right of action has led to an increase in litigation.[169] Under the CCPA, however, an individual may only bring an action if a data breach compromised their personal data, which is much narrower in scope than BIPA.[170] This essentially means that an individual cannot bring an action against a company for violating the CCPA itself by misusing or inappropriately disclosing consumer data.[171] In an attempt to challenge this provision, some consumers have filed suit alleging violations of the CCPA's privacy provisions and arguing that these suits should be allowed to proceed.[172]

The broad scope of the CCPA, in that it protects against various types of consumer data, once again complicates the biometric privacy landscape for private companies who are fighting for compliance by creating an additional set of requirements to satisfy when processing and collecting consumer data. Furthermore, companies that are not within the reach of BIPA, because they are not operating their business

---

165 Graham, *supra* note 123, at 948.

166 *See* David Stauss & Mike Summers, *How Do the CPRA, CPA & VCDPA Treat Biometric Information?*, HUSCH BLACKWELL: BYTE BACK (Feb. 2, 2022) https://www.bytebacklaw.com/2022/02/how-do-the-cpra-cpa-vcdpa-treat-biometric-information.

167 *Id.*

168 Jena M. Valdetero & David A. Zetoony, *CCPA Litigation Up 44.1%*, THE NAT'L L. REV. (Mar. 7, 2022), https://www.natlawreview.com/article/ccpa-litigation-441.

169 *See id.*

170 CAL. CIV. CODE § 1798.150 (West 2023); *cf.* 740 ILL. COMP. STAT. 14/20 (2023) (providing individuals with a private right of action to sue for violations of the statute).

171 Robert Bateman, *The CCPA/CPRA's Private Right of Action*, TERMSFEED, https://www.termsfeed.com/blog/ccpa-private-right-action (July 1, 2023).

172 Valdetero & Zetoony, *supra* note 168.

in Illinois, may still fall under the scope of the CCPA, resulting in a new number of provisions to comply with.[173] The uncertainty regarding the status of the private right of action under the CCPA only conflates this confusion.

Lastly, California is not alone in its quest to create a comprehensive privacy law; states like Virginia, Colorado, Connecticut, and Utah have also enacted comprehensive privacy laws.[174] Though these laws have similarities, like the right to access and delete personal information and to opt out of the sale of personal data, there are still differences within these state laws, again contributing to the complicated landscape surrounding biometric privacy.[175]

C. *Biometric Privacy Under the European Union's General Data Protection Regulation*

The European Union's General Data Protection Regulation (GDPR) is considered the "toughest privacy and security law in the world."[176] It came into effect in 2018, and it places requirements on organizations all over the world, so long as they are collecting the data of people living in the European Union (EU).[177] The GDPR provides expansive protection for the collection of consumer data, including biometric data.[178] Biometric data is covered under personal data, but the GDPR defines it specifically 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."[179] Biometric data is defined broadly

---

[173] *See* Jeffrey N. Rosenthal et al., *Analyzing the CCPA's Impact on the Biometric Privacy Landscape*, LEGALTECH NEWS (Oct. 14, 2020, 7:00 AM), https://www.law.com/legaltechnews/2020/10/14/analyzing-the-ccpas-impact-on-the-biometric-privacy-landscape.

[174] *State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEG., https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy (June 7, 2022).

[175] *Id.*

[176] Ben Wolford, *What Is the GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr (last visited Dec. 19, 2023).

[177] *Id.*

[178] *Id.*

[179] Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1, 34 (EU).

under the GDPR, which may be a sign of an implicit understanding that biometric data and technology is continuing to evolve.[180]

Importantly, the GDPR provides special protection for biometric data.[181] Biometric data is considered sensitive data, and processing is only allowed for certain purposes.[182] Article 6 of the GDPR lists explicit instances in which the processing of sensitive data is allowed.[183] Some examples of when biometric data processing is permitted are as follows: when necessary to enter into a contract with a data subject, when complying with a legal obligation, and when the data subject provides "specific, unambiguous consent."[184] The GDPR requires that the individual provide explicit consent prior to processing and identifies what is meant by consent, which must be informed, freely given, and unambiguous.[185] A company that wishes to request consent should be clear and distinguishable from other issues, so that the individual completely understands what the individual is consenting to.[186] The GDPR "gave governments broad authority to impose fines of up to 4 percent of a company's global revenue, or to force changes to its data-collection practices."[187]

Though the law has been called one of the toughest privacy laws in the world, some have been disappointed with its application—or lack thereof.[188] For example, in 2020, the GDPR penalized Google for a violation, the only major tech organization in the two years since the GDPR's enactment.[189] On the other side of this argument though, is the fact that several giant companies, including Facebook and Google, have created new privacy policies to comply with the expectations of the GDPR.[190] It has also increased user awareness of privacy, which

---

180 *See* Danny Ross, *Processing Biometric Data? Be Careful, Under the GDPR*, IAPP (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr.

181 *Id.*

182 *Id.*

183 Wolford, *supra* note 176.

184 *Id.*

185 *Id.*

186 *Id.*

187 Adam Satariano, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, N.Y. TIMES, https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html (Apr. 28, 2020).

188 *See id.*

189 *Id.*

190 *Id.*

many consider to be a win for the GDPR.[191] For example, Amazon has created a privacy page for consumers where they may learn more about the data that the company is collecting.[192]

D. *Proposed Federal Legislation Surrounding Biometric Privacy Laws*

As the presence of technology in society continues to increase, and consumers become wary of their own data privacy, federal privacy regulation becomes increasingly necessary. Both biometric-specific privacy laws and comprehensive privacy laws have been discussed on a federal level, yet neither has garnered enough political support to be enacted into law.[193] This Part discusses both the biometric-specific privacy law and the comprehensive privacy law that have been introduced by federal lawmakers in recent years and highlights important components of each law that will be necessary for future consideration.

In August 2020, Senators Jeff Merkley and Bernie Sanders introduced federal biometric privacy legislation to Congress.[194] The act, called the National Biometric Information Privacy Act of 2020, would have required private companies to obtain consumers' consent prior to the collection of biometric data.[195] Under this bill, the term "biometric data" included "eye scans, voiceprints, faceprints, and fingerprints."[196] Similarly to BIPA, this act would have created a private right of action for individuals.[197] Additionally, the bill contained a right of access for individuals to know what information a corporation has collected and stored.[198] The senators introduced the bill in response to growing privacy concerns surrounding biometric data and concern over the disproportionate implications for Asian and Black

191 *Id.*

192 *Id.*

193 *See infra* notes 194–203 and accompanying text.

194 Press Release, Jeff Merkley, Senator, Senate, Merkley, Sanders Introduce Legislation to Put Strict Limits on Corporate Use of Facial Recognition (Aug. 4, 2020) [hereinafter Merkley Press Release], https://www.merkley.senate.gov/news/press-releases/merkley-sanders-introduce-legislation-to-put-strict-limits-on-corporate-use-of-facial-recognition-2020.

195 *Id.*

196 *Id.*

197 *Id.*

198 *Id.*

individuals.[199] Though the bill was not enacted into law, it is possible that certain provisions of the bill may be used going forward; therefore, the future of a biometric-specific privacy law on a federal level remains unknown.[200]

The House Energy & Commerce Committee (E&C) advanced a comprehensive privacy law—with bipartisan support—on July 20, 2022.[201] The American Data Privacy and Protection Act (ADPPA) is a notable step for those who have been fighting to create an all-encompassing privacy framework that would protect Americans' personal data in the face of "Big Tech."[202] This bill lists seventeen enumerated purposes for which companies would be allowed to collect and use consumer data, including "things like authenticating users, preventing fraud, and completing transactions."[203] Outside of this list, data processing is prohibited.[204] By creating a specific list of permitted processing purposes, the ADPPA is similar to the GDPR, as discussed above.[205]

Like the GDPR, the ADPPA would emphasize a data-minimization approach, meaning that entities could not collect more data than is necessary while informing consumers about the reason behind

---

199 *Id.*; *see also* Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SITN (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology (discussing the inaccuracy of facial recognition technology among Black individuals and the inequitable application of such technologies).

200 *See* Dmitry Shifrin & Mary Buckley Tobin, *Past, Present and Future: What's Happening with Illinois' and Other Biometric Privacy Laws*, THE NAT'L L. REV. (May 28, 2021), https://www.natlawreview.com/article/past-present-and-future-what-s-happening-illinois-and-other-biometric-privacy-laws; *S. 4400 (116th): National Biometric Information Privacy Act of 2020*, GOVTRACK, https://www.govtrack.us/congress/bills/116/s4400 (last visited Dec. 19, 2023). Senator Merkley introduced the bill in August of 2020, but it died in the 116th Congress. *Id.*

201 *The American Data Privacy and Protection Act*, AM. BAR ASS'N (Aug. 30, 2022), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl.

202 *Id.*

203 Gilad Edelman, *Don't Look Now, but Congress Might Pass an Actually Good Privacy Bill*, WIRED (July 21, 2022, 8:00 AM), https://www.wired.com/story/american-data-privacy-protection-act-adppa.

204 *Id.*

205 *See supra* notes 182–84 and accompanying text.

collection.[206] In light of the concern that consumers lack the requisite knowledge regarding the use of their own data, this provision would appear to be a major success for a federal privacy law. But one major downfall of the ADPPA is that a permitted reason for collecting data is targeted advertising, which is an issue that many data privacy supporters argued against.[207] There are limits, however, to the collection of data for targeted advertising purposes; the law would "ban targeting ads based on 'sensitive data.'"[208] Furthermore, biometric data is included under the definition of "sensitive data."[209] Under the ADPPA, biometric information would be defined as:

> [A]ny covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual including—(i) fingerprints; (ii) voice prints; (iii) iris or retina scans; (iv) facial mapping or hand mapping, geometry, or templates; or (v) gait or personally identifying physical movements.[210]

The ADPPA will likely "apply to certain mHealth apps because the legislation defines 'covered entity' to include entities that determine the purposes and means of collecting, processing[,] or transferring data and are subject to the [FTCA]."[211] This may decrease some of the confusion the various federal privacy statutes (such as HIPAA, COPPA, and others) have created by only applying to specific industries or scenarios. Despite the ADPPA's potential success, the bill has not been enacted into law as of 2023, and its path forward appears to be a tenuous one.[212]

---

[206] Carina Schalhofer, *ADPPA vs GDPR: Comparing Their Scope and Principles*, PRIVIQ (Oct. 27, 2022, 4:22 PM), https://www.priviq.com/blog/adppa-vs-gdpr-comparing-their-scope-and-principles.

[207] Edelman, *supra* note 203.

[208] *Id.*

[209] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(24)(A)(iv) (2022).

[210] § 2(3)(A).

[211] Ehrenkranz et al., *supra* note 87 (alteration in original).

[212] *See* Steve Alder, *Revised American Data Privacy and Protection Act Due to be Released*, HIPAA J. (Apr. 14, 2023), https://www.hipaajournal.com/revised-american-data-privacy-and-protection-act-due-to-be-released ("The March 1, 2023, Committee [on Energy and Commerce] hearing restarted the discussion about federal privacy legislation . . . . There was consensus among subcommittee members that federal privacy legislation is required, and that the ADPPA could well be the path forward. That said, there are different views on what privacy legislation should include and it

IV. SOLUTIONS TO RESOLVING BIOMETRIC PRIVACY CONCERNS ON A FEDERAL LEVEL: LOOKING THROUGH THE LENS OF MOBILE APPS

The current legal framework surrounding biometric privacy has proved unworkable and complicated, making it extremely difficult for consumers to retain control over their biometric data. A comprehensive privacy law, rather than a biometric-specific privacy law, would better serve the American people by prioritizing the right of consumers in maintaining control over their data, while simultaneously acknowledging and balancing the practical benefits of biometric authentication for security purposes. In creating such a law, Congress should consider factors such as the complex and varying definitions of "biometric data," the sensitive nature of biometric data, a comprehensive list of ways in which data can be used, as well as a private right of action with a clear and definitive scope. Finally, a comprehensive privacy law should preempt state privacy laws that directly conflict with federal law, in order to decrease the confusing legal landscape that currently exists and to provide protection for all consumers. Still, state laws with additional data privacy protections in place for consumers should remain.

Section A analyzes how a biometric-specific privacy law would operate on a federal level and highlights its advantages and disadvantages. Section B discusses how a comprehensive privacy law would better serve the federal government's interests, as well as provide better protection for consumers.

A. *Weighing a Biometric-Specific Privacy Law Against a Comprehensive Privacy Law*

As discussed in Part III, senators introduced the National Biometric Information Privacy Act in 2020 in an effort to control private companies' collection of biometric data, and the ADPPA was proposed in recognition of growing concerns surrounding data privacy more generally.[213] Arguments for a biometric privacy law on a federal level point to the fact that the current status of state laws creates a confusing and difficult landscape to maneuver, as companies have to tailor privacy policies to the laws of each state.[214] Supporters also argue

---

was clear that significant changes are needed for ADPPA to stand a chance of being signed into law."); *The American Data Privacy and Protection Act*, *supra* note 201.

[213] *See supra* notes 194–207 and accompanying text.

[214] *See* Simons, *supra* note 13, at 1127 (discussing how a federal biometric privacy law would address the issues posed by BIPA as well as the increasing advancement of biometric technology).

that the inconsistencies between state biometric privacy laws in defining biometric identifiers and debates regarding standing would be best addressed by a federal biometric privacy law.[215] This point is well-taken; yet, this same argument also lends support to creating a comprehensive and generalized federal privacy law, which would address these concerns surrounding BIPA and other state laws, as well create a blanket layer of protection for all consumer data. Adding another too-specific law to the landscape may aggravate some of the compliance issues that society can see through the lens of mHealth apps.

On this same note, however, there may also be concerns that a broad privacy law—like the GDPR—would lead to overregulation due to the amount of information that it would cover. Protecting consumer privacy, however, should be the priority, and it is more important to be overly inclusive in the face of private companies collecting personal data. Furthermore, a comprehensive privacy law would assist private businesses in creating more narrow and tailored privacy policies, whereas the current state of privacy laws leaves too many gaps open for businesses to take advantage of. In fact, experts in favor of a comprehensive federal data privacy statute support the idea that the US government's failure to pass a law that encompasses all industries impacts big business and large entities—those struggling to address the several state and federal privacy laws that implicate various industries.[216] At the moment, some companies choose to focus their compliance on what appears to be the easiest solution and pay fines for laws and regulations that they disregard in the process, rather than dealing with separate laws that have conflicting requirements.[217] A comprehensive privacy law that preempts state law would both decrease this confusion and provide sufficient guidance to companies regarding the use of all consumer data.

Some argue that biometric information is so unique—specifically facial scans collected by facial recognition technology—that the use of such technology by private companies should be banned altogether.[218]

---

[215] *See id.* at 1101, 1128.

[216] *See* Roy Wyman & Colton Driver, *A Federal Data Privacy Law Is the Disaster We Urgently Need*, LAW360 (Aug. 24, 2022, 3:52 PM), https://www.law360.com/articles/1523846/a-federal-data-privacy-law-is-the-disaster-we-urgently-need.

[217] *See id.*

[218] *See* Lindsey Barrett, *Ban Facial Recognition Technologies for Children—And For Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223, 228, 230 (2020).

Though this perspective may take an aggressive approach to protecting biometric data collected by facial recognition technology, it poses a critical consideration: is biometric data so unique and unchanging as to make its collection by private companies too dangerous to allow? This is not the case, as the advantages of biometric technology for security and authentication purposes have proved successful in light of the risks, but it lends support to the fact that biometric information has been used vastly outside of its intended scope. In sum, biometric data has valid and significant uses in the field of data privacy and security; it is only when biometric data is used outside of its original use that consumers should be wary of its purpose, and federal lawmakers should focus their attention.

Although biometric privacy is of heightened concern, due to its unique nature, a comprehensive privacy law may be better suited for the state of technology today. Mobile apps collect several types of data from users, and biometric data is just one area of concern.

B. *Drafting a Comprehensive Federal Privacy Law*

The rapidly changing biometric privacy landscape—alongside the ever-evolving use of biometric technology—supports the argument that the most effective solution is a comprehensive privacy law. Such a law will prove the most beneficial for both consumers, who are sharing their data in a constantly changing technological world, and for private companies, who are navigating the complicated privacy landscape. There are several components that a federal comprehensive law must include. First, as discussed in Subsection 1, federal legislators should focus on data minimization, which would limit the collection of data to necessary purposes,[219] and create a clear explanation of the permissible uses of data. This would also require the informed consent of the consumer prior to use that is outside the list of permitted uses, which must specify exactly what the data is being used for, and how long the company intends to retain the data. Along with data minimization, biometric data should be subject to heightened protections under the law, meaning that there should be additional requirements satisfied in order to process biometric data, such as informed consent. Similarly, the term "biometric identifier" should be broadly defined to account for the fact that biometric technology continues to evolve, and different methods of biometric data collection

---

[219] Mohammed Khan, *Data Minimization—A Practical Approach*, ISACA (Mar. 29, 2021), https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach; *see infra* notes 222–30 and accompanying text.

may emerge in the future. Second, as discussed in Subsection 2, a privacy law must include a private right of action to permit the consumer to seek out a remedy against any private company who fails to protect their data.[220] Finally, as discussed in Subsection 3, the scope of the privacy law must be broad and should not be confined to commercial purposes, as there are many uses for biometric data which hold similar risks, even when they are not used by private businesses.[221]

1. Data Minimization, Heightened Protection, and Informed Consent

The principle of data minimization, the requirement of special protections for biometric data, and the necessity of informed consent are three crucial components of a comprehensive privacy law. These components provide better protection for all forms of consumer data, while adding an additional layer of security for biometric data.

First, a comprehensive privacy law must prioritize data minimization, meaning that the company or entity should be required to collect only what is necessary in order to provide the service.[222] For example, when companies use biometric data to authenticate users and provide an additional level of security for personal information, this should be considered a "necessary" use. The use and collection of biometric data for a commercial purpose, however, such as benefitting a business's AI technology, as was the case with J&J's app, Neutrogena Skin360, should not be considered "necessary" under the law.[223] Entities should be required to limit the use of biometric data to "necessary" purposes unless they have the individual's informed consent for broader uses.

The principle of data minimization is also an important part of the GDPR, which states that, "[p]ersonal data shall be: . . . adequate, relevant[,] and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."[224] A US comprehensive privacy law should copy similar language to emphasize that such data should only be used for permitted purposes. For example, as discussed in Part II, biometric authentication and identification has proved advantageous for cybersecurity by providing

---

220 *See infra* notes 231–37 and accompanying text.

221 *See infra* notes 238–42 and accompanying text.

222 Khan, *supra* note 219.

223 *See supra* notes 136–40 and accompanying text.

224 Council Regulation 2016/679, art. 5, 2016 O.J. (L 119) 1, 35 (EU).

consumers with an extra level of protection.[225] By emphasizing data minimization as a foundational principle behind a comprehensive privacy law, the focus is more on the protection of consumers rather than on the protection of big businesses, which is a necessary piece in giving control back to the individual.

Second, a comprehensive privacy law must provide special protection for biometric data. Classifying biometric data as sensitive personal data adds an extra layer of protection by ensuring that data is not used outside of necessary purposes unless the consumer provides explicit consent. As discussed in Part II, biometric data is both sensitive and unique, as it is forever linked to the individual to whom it belongs.[226] Mobile apps provide insight into how data can be used outside of its intended purpose; therefore, as discussed above, federal privacy legislation should take a data minimization approach and restrict the use and collection of biometric data to approved and permitted uses, absent users' informed consent. Permissible purposes should include security, such as authentication and identification, government and public interest purposes, and health and safety purposes. Outside of these identified lawful bases, the organization must obtain the informed consent of the consumer, as discussed below. In sum, a comprehensive privacy law should include biometric data as "sensitive personal data" and permit the collection and processing of such data only for permissible purposes, as outlined above.

Additionally, the definition of biometric data under the ADPPA, as discussed in Part III, suggests that data identified under "biometric data" is not an exhaustive list, which acknowledges that biometric technology is always changing.[227] The CCPA takes a similar approach in its definition of biometric data, creating a long and expansive list of potential biometric identifiers, and including both physical and behavioral characteristics.[228] In consideration of biometric technology's potential to advance, a definition of "biometric identifiers" similar to that of the ADPPA and the CCPA is a necessary component of any future comprehensive privacy law. For example, the definition of biometric identifiers under the federal privacy law should seek to include the identifiers that have been incorporated in the

---

225 *See* discussion *supra* Part II.A.

226 *See supra* notes 8–11 and accompanying text.

227 *See* discussion *supra* Part III.D.

228 *See supra* notes 163–65 and accompanying text.

various state laws, such as facial prints, iris scans, and fingerprints, to name a few.[229] Additionally, behavioral characteristics, such as gait and mannerisms, and other personally identifying human characteristics must be included within the definition. Finally, the definition should explicitly state, however, that the list is not exhaustive, in an effort to recognize that biometric technology is ever evolving.

Following the approach of data minimization, obtaining the informed consent of consumers is crucial to ensure that consumers are aware of the ways in which data can be used. Outside the list of approved uses, as discussed above, individuals must consent to their data collection and use in order for a company to process biometric data. Experts argue that the issue, however, is that it is time consuming and even boring for consumers to constantly review privacy policies to see what organizations are doing with their data.[230] Therefore, even with a consent or notice requirement, individuals may nevertheless simply accept to avoid getting wrapped up in reading privacy policies with language that is full of legalese and technological language. Still, consumers must be adequately informed about data use and their right to data privacy. To combat the issue of confusing privacy policies, a federal privacy law should be explicit, in clear and unambiguous terms, regarding the ways in which privacy policies should be written. Privacy policies should also avoid confusing and misleading language, providing in simple terms what data the company intends to collect, how it intends to use such data, and how long it intends to keep such data.

While individuals should have a right to consent to the collection and use of personal data, consent is not the sole answer to privacy. Therefore, informed consent, along with more stringent restrictions on the processing of biometric data, must be put in place to prevent the misuse of biometric data.

2. A Private Right of Action

A private right of action must be on the agenda for any future federal privacy legislation. There is controversy over the scope of a private right of action following BIPA, which some argue causes "meaningless litigation."[231] The increase in litigation surrounding BIPA is likely due to the low standing threshold, as decided by the

---

229 *See* discussion *supra* Part III.B.

230 *See* Wyman & Driver, *supra* note 216.

231 *See id.*

Supreme Court of Illinois in *Rosenbach*, whose "[o]pponents . . . reasonably fear that a wave of frivolous lawsuits" and a substantial hike in class actions would follow that decision.[232] But this standing issue may have more to do with the interpretation of an "aggrieved party" under the Supreme Court of Illinois' holding in *Rosenbach*, and less to do with the language of BIPA itself.[233] Others argue that the flow of litigation is due to plaintiffs' ability to "seek actual or liquidated damages of either $1,000 per negligent violation or $5,000 per intentional or reckless violation."[234]

On the other hand, some argue that the private right of action in BIPA provides "the ultimate layer of protection for the . . . consumer" by allowing individuals to sue companies directly who misuse the biometric information that they collect.[235] Given the unique nature of biometric data, and the potential for its misuse, a private right of action is a necessary component of a comprehensive privacy law because it provides individuals with recourse when their data is misused. While the private right of action under BIPA has paved the way for many lawsuits against businesses, it is nevertheless necessary in order for consumers to have full control over their data.

When looking towards a federal privacy measure, a private right of action is necessary to strike the balance of keeping companies accountable while allowing the advancement of biometric technology. Congress should explicitly define how an individual must establish standing in order to pursue any action. For example, an individual must allege exactly how their data was misused and how the company violated federal law in processing the data. Importantly, individuals must prove how data misuse may cause harm and define what potential damages will flow from the harm, in order to have recourse under the private right of action. Individuals should not be required to show actual harm, as this may prove burdensome and will take away control

---

232 Metzger, *supra* note 17, at 1090; *see also* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1200 (Ill. 2019).

233 *See* Metzger, *supra* note 17, at 1079 ("[T]he court held a person is 'aggrieved' when there is a technical violation of BIPA; a showing of further harm is not necessary to bring a cause of action under the statute.").

234 Fredric D. Bellamy, *Looking to the Future of Biometric Data Privacy Laws*, THOMSON REUTERS (Apr. 6, 2022, 10:13 AM), https://www.reuters.com/legal/legalindustry/looking-future-biometric-data-privacy-laws-2022-04-06.

235 Carla Llaneza, Comment, *An Analysis on Biometric Privacy Data Regulation: A Pivot Towards Legislation Which Supports the Individual Consumer's Privacy Rights in Spite of Corporate Protections*, 32 ST. THOMAS L. REV. 177, 184 (2020).

from the consumer, which is contradictory to the purpose of a private right of action.

Unlike the CCPA, however, a private right of action should not only be available to an individual when there is a data breach. Instead, a future privacy law should provide standing to individuals whenever they can allege that a company or an organization has violated a section of the privacy law, and that the company has misused the data in such a way that is certain to cause harm. Damages awarded to the consumer are appropriate because the business is explicitly violating the law and jeopardizing the security of the consumer by processing their data without informed consent. Data breaches are a genuine concern, and biometric data has the potential to be misused in the hands of the company collecting it, outside of any hackers or cybercriminals. This provision is necessary to leave ultimate control with consumers.

Finally, in comparing Texas's CUBI and BIPA, more companies have been held responsible for improper data use when individuals have a private right of action, compared with Texas, where discretion is left with the attorney general.[236] As discussed earlier in Part III, the Texas attorney general has only recently begun to exercise its power in enforcing the state's biometric privacy law.[237] This has taken some power away from Texans and may be less of a deterrent factor for private companies if the law is not being adequately enforced.

3. The Scope of a Comprehensive Privacy Law

In defining the scope of a comprehensive privacy law, a good place to start is the GDPR. It is argued that the GDPR benefits private businesses by providing a compliance framework that accounts for cybersecurity concerns, improves management of data, and refines consumer loyalty and trust.[238] In providing explicit requirements for data use, however, the GDPR also provides protection for citizens of the EU. Furthermore, the GDPR has served as a privacy model for countries like Brazil, Japan, and India—to name a few—as well as the

---

[236] *See supra* notes 145–51 and accompanying text.

[237] *See supra* notes 145–51 and accompanying text.

[238] *See, e.g.*, Michael Fimin, *Five Benefits GDPR Compliance Will Bring to Your Business*, FORBES (Mar. 29, 2018, 7:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business.

United States, indicating its workable framework for a US privacy law.[239]

A comprehensive federal privacy law should follow the GDPR in its application and scope. The GDPR applies to businesses, public bodies, institutions, and nonprofit organizations, while other privacy laws, like the CCPA, only apply to private businesses.[240] This is a notable advantage of the GDPR, whose broadness ensures that consumers have data protection regardless of whether the organization is for-profit, or not.[241] Of course, a comprehensive privacy law may include exceptions; for example, the Department of Homeland Security may not be held to the same standard as private companies in its collection of biometric data, because the governmental interest in providing for national security is more of a necessity than a private business's interest. Furthermore, the GDPR applies when companies process the personal data of both EU citizens and residents, so if a company plans to provide services to citizens or residents, then the GDPR will apply.[242] A US privacy law should be similar to the GDPR in scope to allow for protection of its citizens from companies who operate outside of the United States.

As seen with the GDPR, a comprehensive privacy law is not without its problems. Because technology is quickly evolving, it is difficult to create a federal law that will predict all the avenues in which technology will go. Still, the protection of individual privacy is too critical, and a comprehensive federal privacy law takes the initial and necessary step toward that protection. To combat the issue of the ever-evolving world of technology, federal lawmakers should aim to keep the comprehensive privacy law broad so that it may adapt to the changing technology, while still prioritizing consumer protection.

V. CONCLUSION

Biometric technology has drastically evolved since the discovery of fingerprints as a method of identification, and it will only continue to do so. With mobile apps intertwined in people's daily lives, society is becoming more comfortable in sharing data with private companies when arguably they should be more wary and skeptical of the ways in

---

239 *See* Satariano, *supra* note 187.

240 ALICE MARINI ET AL., DATAGUIDANCE & FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR V. CCPA 7 (2018), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

241 *See id.*

242 *See* Wolford, *supra* note 176.

which their data is actually being used. As previously discussed, contact tracing apps depict one way in which biometric data has been used outside the scope of users' understanding.[243] Companies using data to benefit their own technological platforms confirms another way in which data is being used outside of its intended scope.[244] Biometric technology is not slowing down; therefore, a comprehensive privacy law that prioritizes the rights of consumers through a data minimization approach, a private right of action, and a broad scope, is necessary to preserve data privacy. Without a concrete privacy law in place on a federal level, consumers' biometric data will continue to go largely unregulated, as this data falls within the cracks of the complex legal landscape that is currently in place in the United States.

---

[243] *See supra* notes 39–53 and accompanying text.

[244] *See supra* notes 136–43 and accompanying text.


SETON HALL UNIVERSITY
HAZARD YET FORWARD
1856