BIOMETRIC PRIVACY AS A CASE STUDY FOR U.S. PRIVACY OVERALL

BY KIRK NAHRA

& ALI JESSANI

& AMY OLIVERO

& SAMUEL KANE

Kirk Nahra is a partner at WilmerHale. He co-chairs the firm's Cybersecurity and Privacy Practice as well as the Artificial Intelligence Practice. Ali Jessani, Amy Olivero, and Samuel Kane are associates at WilmerHale.

Visit www.competitionpolicyinternational.com for access to these articles and more!

BIOMETRIC PRIVACY AS A CASE STUDY FOR U.S. PRIVACY OVERALL

By Kirk Nahra, Ali Jessani, Amy Olivero & Samuel Kane

Privacy law in the United States is best described as a patchwork of rules and regulations at both the state and federal level. This development is perhaps no better exemplified than by how the U.S. regulates biometric information. From competing definitions to (sometimes) contradictory compliance obligations, the rules surrounding the processing of biometric information are myriad and complex, creating meaningful challenges for companies that wish to take advantage of the benefits associated with processing it (which include increased security and more convenience for consumers). This article outlines how the rules governing biometric data reflect U.S. privacy at large and how this approach negatively impacts both consumers and businesses.

01
INTRODUCTION

Privacy law in the United States has long stood out as a uniquely complex legal landscape. In the absence of a comprehensive federal law regulating privacy (such as exists in Europe with the General Data Protection Regulation, or "GDPR"), what has emerged instead is a complicated mix of legal and regulatory frameworks. Some states, for instance, have passed comprehensive privacy laws that seek to broadly regulate the collection and use of consumer data across sectors. Meanwhile, other federal and state laws take on narrower privacy challenges, focusing specifically on particular types of data or privacy practices within specific sectors. And against the backdrop of these statutory frameworks, federal and state regulators have made their own attempts to bring uniformity to the way that companies use consumer data.

The regulation of biometric information exemplifies the complicated nature of U.S. privacy law writ large. As in the broader privacy landscape, there is no single legal framework that comprehensively regulates biometric privacy. Rather, biometric privacy falls within the purview of numerous legal frameworks—from efforts of federal regulators like the Federal Trade Commission ("FTC") and federal sector-specific laws, like the Health Insurance Portability and Accountability Act ("HIPAA"), to biometric-specific privacy laws at the state level, like the Illinois Biometric Information Privacy Act ("BIPA"), and state comprehensive privacy laws. This legal complexity, in turn, creates challenges for (1) companies seeking to comply with an increasingly convoluted—and at times overlapping—landscape of requirements surrounding the use of biometric data; (2) regulators seeking to use their enforcement authority in the biometric privacy sphere; and (3) individuals seeking to understand what rights they have in relation to their biometric data.

This article seeks to shed light on the complex tangle of laws governing the collection and use of biometric data, and in doing so, offer useful insights for companies, regulators, and individuals seeking to understand how the laws and regulations interact with each other. After briefly explaining the unique privacy challenges presented by biometric data and providing a general overview of how biometric data is defined under various legal frameworks, this article moves into a discussion of the spectrum of U.S. legal requirements governing the collection and use of biometric data, including the enforcement activities of the FTC, federal laws focused on particular types of biometric-adjacent data, state biometric privacy laws, state comprehensive privacy laws, and sector-specific state laws.

01
RECOGNIZING THE IMPORTANCE OF BIOMETRIC DATA PRIVACY

Biometric data is playing an increasingly prominent role across many areas of society. In the public sector, for example, criminal and immigration databases track individuals' fingerprints, and law enforcement agencies deploy facial recognition technology ("FRT") to identify malicious actors. Private sector companies, meanwhile, increasingly use biometric data for authentication and verification purposes, offering alternatives to traditional PINs or passwords and greater convenience for consumers. (Consider the ubiquity of the fingerprint and/or facial scan unlock capability on smartphones and personal computers as an example.) This technology is often seen as more efficient, cost-effective, and user-friendly than traditional methods, while also providing a more secure and less user error-prone alternative to passwords.

Despite these advantages, however, the collection, use, storage, disclosure, and analysis of biometric data also raise significant privacy concerns given the immutable and highly identifiable nature of biometric data. Unlike a password, PIN, or even SSN, data like fingerprints, facial features, and iris scans cannot be changed if they become compromised. Biometric information can also be abused and illegitimately used to produce counterfeit videos or voice recordings ("deepfakes") meant to impersonate individuals for fraudulent or harassing purposes.

The national spotlight has focused on biometric data privacy in recent years as lawsuits alleging violations of BIPA, Illinois's biometric data privacy law, have surged.[2] This rapid increase in legal activity, coupled with continuing technological innovation, has brought biometric privacy onto the

2 Then-governor Rod Blagojevich signed BIPA into law in 2008. The law remained quiet for many years until a landmark Illinois Supreme Court decision in 2019. That case, Rosenbach v. Six Flags, highlighted the power of the law's private right of action by holding that a violation of BIPA is considered a per se violation. In other words, in a BIPA lawsuit, the plaintiff does not need to plead actual harm or injury from the violation in order to successfully plead. *See generally* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019). Since that case, over 1,500 BIPA lawsuits have been filed. *See* Kristine Argentine & Paul Yovanic, *Privacy in Focus: BIPA's Current Landscape and the Crucial Role of Statutory Exemptions*, JDSupra (Feb. 18, 2024), https://www.jdsupra.com/legalnews/privacy-in-focus-bipa-s-current-7659939/.

national stage, raising questions about how companies and governments use this data, what safeguards exist to protect individual privacy, and how these protections translate into legal obligations for companies.

02
DEFINING "BIOMETRIC DATA"

Although the laws and regulations define "biometric information" or "biometric data" differently, there are some general similarities and trends across jurisdictions. Broadly speaking, biometric data can be defined in two main ways: (1) based on the source of the data itself and/or (2) based on the processing activity or capability—namely, whether the data can be used to identify an individual.[3] Most statutes require both elements to be present for a piece of data to qualify as "biometric data" within the scope of protection.

When considering the source of biometric data, most biometric and comprehensive privacy laws focus on these main forms of information from the source individual:

- Retina or iris scans,
- Fingerprints,
- Voiceprints[4],
- Hand scans, and
- Face scans.[5]

Various U.S. federal agencies,[6] current biometric privacy laws, and regulatory guidance limit the scope of biometric information to only personal information that can be used to recognize, identify, or verify an individual.[7] This limitation in definitional scope suggests that these laws are primarily concerned with regulating the physiological characteristics that can be distinctively associated with unique individuals. Many BIPA lawsuits also raise this critical question of whether certain categories of biometric data are capable of identifying individuals such that they are regulated under the law.[8] For example, in a recent case, a federal district court concluded that even though BIPA asserts an exclusion for photographs, the information collected and stored by a defendant constituted "biometric information" within the scope of the statute because the defendant used algorithms to extract and analyze the geometry of faces in the photos it stored.[9]

Put all together, a definition of biometric information can look like the language enacted in Virginia's Consumer Data Protection Act ("VCDPA"): "Biometric data is 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. [It] does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA."[10]

3 See Tatiana Rice, *When is a Biometric No Longer a Biometric?*, Future of Privacy Forum (May 19, 2022), https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/ (providing this simple breakdown of the definition).

4 Voiceprints are a digital model of an individual's unique way of speaking. See e.g. R L Brunelle & F A Lundgren, *Speaker Identification by the Voiceprint Method,* 322 International Criminal Police Review 250 (Nov. 1978), https://www.ojp.gov/ncjrs/virtual-library/abstracts/speaker-identification-voiceprint-method (explaining one voiceprint technique that uses variations in pronunciation of words and phrases to produce a graphic display of frequency over time that is unique to an individual).

5 These definitions commonly exclude data such as digital or physical photographs, audio recordings, and "any data generated from a… video recording. See e.g.4 Colo. Code Regs. § 904-3-2-02

6 See generally definitions provided on the official government agency websites for the National Institute of Standards and Technology, Federal Bureau of Investigation, and Department of Homeland Security.

7 The only state comprehensive or biometric privacy law that does not explicitly necessitate an identification capability for biometric data is Texas's Capture or Use of Biometric Identifier Act. *See* Tex. Bus. & Com Code Ann. § 503.001(a) (defining "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry").

8 See *Bell v. Petco Animal Supplies Stores, Inc*., No. 1:22-cv-06455 (N.D. Ill. 2022) (finding that the critical fact to survive a motion to dismiss was whether the voice data that Petco collected from its employees was capable of identifying someone, not whether Petco used the data for that purpose).

9 See *Rivera v. Amazon Web Servs., Inc*., No. 2:22-CV-00269, 2023 WL 4761481 (W.D. Wash. July 26, 2023).

10 VA Code Ann. § 59.1-575 (2021).

03

UNDERSTANDING THE LEGAL AND REGULATORY FRAMEWORKS GOVERNING BIOMETRIC PRIVACY

A. FTC Enforcement

Similar to general data privacy rights, privacy rights for biometric data are defined through specific provisions in laws and regulatory actions that dictate how companies should collect, store, process, disclose, and dispose of data. The FTC is the federal regulator that most consistently pursues biometric information as an enforcement priority. The agency primarily relies on its enforcement authority under Section 5 of the FTC Act — through which it regulates "unfair" or "deceptive" acts or practices — to bring these types of cases. Its enforcement authority under the law has remained malleable enough to empower the agency to maintain its consumer protection mission across new and emerging industries and use cases.

In May 2023, the FTC published a policy statement declaring that it is "committed to combatting unfair or deceptive acts and practices related to the collection and use of consumers' biometric information and the marketing and use of biometric information technologies."[11] In this policy statement, it articulated a broad definition of biometric information, encompassing not just images, descriptions, and recordings of an individual's facial features, iris/retina, fingerprint, handprint, voice, genetics, or characteristic movements, but also "data derived from such depictions" to the extent that it could be used to identify a person.[12] This definition is notably broader than most definitions of "biometric information" asserted in state laws, which tend to exclude photos, videos, and audio recordings and data generated from those sources.

The policy statement describes examples of business practices using consumer biometric data that the FTC would likely consider not in compliance with Section 5 of the FTC Act. The FTC asserts, for example, that practices like making "false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information"[13] place honest vendors at a competitive disadvantage and could result in consumer harms such as wrongful denial of benefits or payment. Companies collecting biometric information should also:

- clearly disclose their practices and not require biometric information in exchange for essential goods and services;[14]
- take reasonable actions to prevent harm and safeguard information, such as conducting security assessments, limiting access to biometric data, and ensuring timely system updates;[15] and
- use the assessments to investigate the extent of any third-party testing, the similarities between the test and production environments, and any disproportionate harm of a particular demographic.[16]

Two years prior to the 2023 policy statement, the FTC initiated an enforcement action against the mobile and web photo app Everalbum.[17] The FTC alleged that Everalbum's photo app default setting to enable face recognition could not be disabled by users outside of jurisdictions with specific biometric data protections (i.e. Texas, Illinois, Washington, and the European Union). According to the FTC, Everalbum misrepresented users' ability to control the app's face recognition feature and also misrepresented the deletion of users' photos upon deactivation, among other allegations. As part of the Final Order, Everalbum had to (1) "clearly and conspicuously disclose" all the purposes for collecting a consumer's biometric data to the consumer (through a separate means from Everalbum's privacy policy

11 Press Release, *FTC Warns About Misuses of Biometric Information and Harm to Consumers*, Federal Trade Commission (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

12 See Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act 1, 1 (2023).

13 *Id.* at 6.

14 *Id.* at 7.

15 *Id.* at 10. FTC enforcement actions, like its 2012 action against EPN, Inc., set the foundation for how the agency assesses companies' security practices for personal data like biometric information. See Complaint, *In re EPN, Inc*., FTC File No. 1123143 (Oct. 3, 2012) (alleging the debt-collecting company failed to assess risks to the consumer personal information that it collected and stored, which resulted in a data breach).

16 *Id.* at 9.

17 See generally Complaint, *In the Matter of Everalbum*, FTC File No. 1923172 (May 7, 2021).

or terms and conditions), and (2) obtain the consumer's affirmative express consent.[18]

The FTC has also shown a strong interest in the potential for bias and discrimination caused by AI using biometric information, as it noted in its complaint against the pharmacy and convenience store Rite Aid.[19] In that action, the FTC charged that Rite Aid unfairly processed its customers' biometric information through use of an in-store facial recognition surveillance system that captured customers' live images and compared it to a database of "persons of interest" to flag for store employees. In associated case documents, the FTC emphasized that consumer-facing applications of AI that use personal and/or biometric data to make automated decisions about an individual must exercise full caution and testing to ensure the technology produces fair and unbiased outcomes.[20] The FTC's regulatory regime, by requiring elevated compliance from companies that collect, process, and/or disclose consumer biometric data, thus establishes some of the strongest current biometric data privacy protections.

B. Other Federal Laws

Mirroring the greater data privacy debate in the U.S., there is no federal comprehensive biometric data privacy law. However, HIPAA provides a set of protections and privacy rights if an individual's biometric data constitutes protected health information ("PHI") within the scope of the law.[21] PHI is defined as "individually identifiable health information" that is processed by a "covered entity" (which is defined to include health care providers,[22] health plans, or health care clearinghouses) or a "business associate" (that is defined as an entity that processes PHI on behalf of a covered entity) and that "relate[s] to the past, present, or future physical or mental health or condition of an individual" in a way that identifies or could identify the individual.[23] Once classified as PHI, biometric data is subject to numerous protections and rights under HIPAA. The rules for covered entities regulated under HIPAA are outlined in the HIPAA Privacy Rule, HIPAA Security Rule, and the HIPAA Breach Notification Rule.

There are also small signals demonstrating a growing interest from federal legislators and executive branch officials in regulating biometric data, specifically. For example, Section 5104 of the Fiscal Year 2021 National Defense Authorization Act tasks the National AI Advisory Committee with advising the President on "whether the use of facial recognition by government authorities . . . is taking into account ethical considerations and . . . whether such use should be subject to additional oversight, controls, and limitations."[24] Additionally, the White House Office of Science and Technology Policy released a Request for Information in October 2021 addressing uses, harms, and recommendations for biometric technologies.[25]

"There are also small signals demonstrating a growing interest from federal legislators and executive branch officials in regulating biometric data, specifically

C. State Biometric Privacy Laws

The most straight-forward way to recognize rights and protections for a specific area is to pass a statute establishing those rights and protections. To date, three states have taken this approach in relation to biometric data: Illinois (BIPA), Texas (the Capture and Use of Biometric Identifier Act ("CUBI Act")), and Washington (the Biometric Privacy Protection Act ("BPPA")).

18 Decision and Order, *In the Matter of Everalbum*, FTC File No. 1923172 (May 7, 2021) at 4.

19 See generally Complaint, *FTC v. Rite Aid*, No. 2:23-cv-5023 (E.D. Pa. Dec. 19, 2023).

20 See Statement of Commissioner Alvaro M. Bedoya on *FTC v. Rite Aid Corporation & Rite Aid Headquarters Corporation*, FTC (Dec. 19, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_commissioner_bedoya_riteaid_statement.pdf.

21 Notably, the Gramm-Leach-Bliley Act ("GLBA") may also provide privacy protections for customer authentication voiceprints that a bank records, as such voiceprints likely fall within the ambit of the "nonpublic personal information" protected by the GLBA. See 15 U.S.C. § 6809(4), 12 C.F.R. § 1016.3(q). The Genetic Information Nondiscrimination Act of 2008 ("GINA") may also provide some protections for biometric information that falls within the scope of protected "genetic information" to the extent it involves information about an individual's genetic tests and health and disease conditions. *See* 42 U.S.C. § 2000ff.

22 But only those that transmit any information in an electronic form in connection with a transaction for which the Department of Health and Human Services has adopted a standard.

23 This explanation is the combination of two definitions in HIPAA: "PHI" and "individually identifiable health information." See generally 42 C.F.R. § 160.103.

24 Pub. L. 116-283, § 5104(e)(2)(A), 134 Stat. 3388 (Jan. 1, 2021).

25 Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Federal Register 56300 (Oct. 8, 2021).

The scope and popularity of BIPA's private right of action sets it apart as the strongest mechanism to uphold biometric privacy rights. BIPA mandates written consent and requires entities to inform individuals about the collection, storage, and use of their biometric information, including the purpose and duration.[26] Biometric information must be destroyed when its collection purpose is fulfilled or within three years of the individual's last interaction with the entity.[27] The Act prohibits selling, leasing, trading, or profiting from a person's biometric information, and it mandates a public written policy for record retention and destruction.[28] For damages, BIPA stipulates $1,000 for each negligent violation and $5,000 for each reckless or intentional violation.[29]

Common allegations under BIPA include issues related to employee timekeeping verification systems,[30] photo tagging on social media,[31] and facial recognition technology.[32] A recent trend has been class action lawsuits against retailers for virtual "try-on" features on websites, which may require facial mapping.[33] Consumers and companies should both be familiar with the most notable BIPA cases and holdings, as they continue to evolve the boundaries of enforceable biometric privacy rights. Some of these precedents include:

- In *Tims v. Black Horse Carriers, Inc.*, the court ruled that individuals have five years to bring claims under BIPA's private right of action.[34]
- In *Apple v. Barnett*, the Illinois appellate court determined that Apple's Face ID on iPhones did not fall under BIPA's requirements because the biometric data is stored on the device and not on Apple's server.[35]
- In *Cothron v. White Castle System, Inc.*, the court held that a separate claim accrues under BIPA each time a private entity scans or transmits an individual's biometric identifier or information in violation of the Act.[36]

The litigation trails for the other two major state biometric privacy laws, Washington's BPPA[37] and Texas's CUBI Act[38], are much shorter than that of BIPA, mainly because they do not include a private right of action. Washington's BPPA prohibits the collection and retention of biometric data for a commercial purpose without providing notice or obtaining consent, and it mandates reasonable data security and destruction policies for biometric data. Similarly, Texas's CUBI Act establishes a notice-and-consent framework that entitles individuals to being informed about and consenting to the collection of their biometric data. It prohibits the disclosure of biometric information with some exceptions, such as for postmortem identification purposes or when another statute permits the disclosure. The CUBI Act also mandates reasonable data security and destruction policies and imposes a civil penalty of up to $25,000 for each violation. In 2022, Texas Attorney General ("AG") Ken Paxton sued Google for allegations that it violated the CUBI Act due to (1) its "Face Grouping" feature that uses facial recognition to create photo records of recurring people in photos in Google Photos, and (2) its Nest platform that records and allegedly creates a voice print of individuals.[39] The case is still ongoing.

26 740 Ill. Comp. Stat. 14/15 (2008)

27 *Id.*

28 *Id.*

29 740 Ill. Comp. Stat. 14/20 (2008)

30 See e.g. *Cothron v. White Castle Sys., Inc*., 216 N.E.3d 918, 929 (Ill. 2023); *Abudayyeh v. Envoy Air, Inc*., No. 20-CV-00142, 2021 WL 3367173 (N.D. Ill. Aug. 3, 2021); Aguilar v. Rexnord LLC, No. 17 CV 9019, 2018 WL 3239715 (N.D. Ill. July 3, 2018).

31 See e.g. *Zellmer v. Facebook, Inc*., No. 3:18-CV-01880-JD, 2022 WL 976981 (N.D. Cal. Mar. 31, 2022); Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019); *Rivera v. Google Inc*., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

32 See e.g. *Hogan v. Amazon.com, Inc*., No. 21 C 3169, 2022 WL 952763 (N.D. Ill. Mar. 30, 2022); *Hazlitt v. Apple Inc*., 543 F. Supp. 3d 643 (S.D. Ill. 2021); *Jacobs v. Hanwha Techwin Am., Inc*., No. 21 C 866, 2021 WL 3172967 (N.D. Ill. July 27, 2021).

33 See e.g. *Warmack-Stillwell v. Christian Dior*, 655 F.Supp.3d 742 (N.D. Ill. 2023); *Kukovec v. Estée Lauder Co., Inc*., No. 22 CV 1988, 2022 WL 16744196 (N.D. Ill. Nov. 7, 2022); *Theriot v. Louis Vuitton North America, Inc*., 645 F.Supp.3d 178 (S.D.N.Y. 2022).

34 *Tims v. Black Horse Carriers, Inc.,* 184 N.E.3d 1029 (Ill. 2022).

35 *Apple v. Barnett*, 225 N.E.3d 602 (Ill.App.1 Dist. 2022).

36 *Cothron v. White Castle Sys., Inc*., 216 N.E.3d 918, 929 (Ill. 2023) (answering certified question from the 7th Circuit).

37 See generally Wash. Rev. Code § 19.375.010 et seq.

38 See generally Tex. Bus. & Com Code Ann. § 503.001 et seq.

39 Press Release, *Paxton Sues Google for its Unauthorized Capture and Use of Biometric Data and Violation of Texans' Privacy*, Office of Attorney General (Oct. 20, 2022), https://www.texasattorneygeneral.gov/news/releases/paxton-sues-google-its-unauthorized-capture-and-use-biometric-data-and-violation-texans-privacy.

D. Comprehensive State Privacy Laws

In addition to targeted laws, comprehensive data privacy laws at the state level also regulate biometric privacy. As of March 2024, each of the fourteen states to successfully enact a comprehensive data privacy bill[40] have a provision declaring biometric information as a form of "sensitive information"—a subcategory of data that receives stronger safeguards and protections, typically because there is an elevated risk of harm or injury to the individual should the data be accessed by an unauthorized person or misused or processed in an unauthorized way.

For example, the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"),[41] addresses biometric information as an element of personal information and further classifies biometric information as "sensitive personal information" when used or intended to be used to identify an individual. In addition to recognizing a general set of individual privacy rights often found in comprehensive privacy laws,[42] businesses must also allow consumers to limit the use of their sensitive personal information to specific purposes.

Other states, such as Colorado, go even further than California and require controllers to obtain affirmative consent prior to processing "sensitive data" (which includes biometric information, albeit with a narrower definition than the one in place in California). State comprehensive privacy laws also often require controllers to conduct and document data protection assessments for the processing of sensitive data, as well as to provide consumers with the right to opt-out of certain automated decision-making activities (which could be implicated by the use of biometrics). Obligations like these ensure appropriate measures are in place to protect individuals' privacy. Overall, these comprehensive data privacy laws reflect a growing recognition of the need to safeguard biometric information and provide individuals with greater control over their personal data.

E. Sector-Specific State Privacy Laws

Biometric privacy rights and protections also pop up in provisions in smaller, sector-specific state laws. These local and state laws illustrate the diverse and evolving landscape of regulations for the commercial use of biometric data and reflect the need for companies to stay vigilant in their compliance efforts under laws such as:

- New York City's Admin. Code, §§ 22-1201 through 1205, which mandates "commercial establishments" collecting biometric information from customers to disclose the collection by placing a "clear and conspicuous sign" near all customer entrances. It also prohibits the sale, lease, trade, share, exchange for anything of value, or other profit from the transaction of biometric identifier information and established a limited private right of action.[43]
- Portland, OR Ordinance Number 190114, which prohibits the use of FRT in places of public accommodation within the city limits. It also establishes a private right of action for any "damages sustained as a result of the violation."[44]

Although the NYC law and Portland ordinance establish private rights of action, these laws will likely have limited impact given their jurisdictional scope. However, there is one sector-specific state law with a private right of action that is expected to cause a more significant disruption in the privacy litigation landscape: Washington's comprehensive health data law, the My Health My Data Act ("MHMDA").[45]

Passed in 2023, the MHMDA aims to protect health information that falls outside the scope of HIPAA. It is a consent-based law: It requires regulated entities to obtain consent for collecting or sharing consumer health data in the first instance[46] and further requires a separate signed authorization from consumers for "selling" "consumer health data" (which includes biometric data). The law is enforceable through Washington's state consumer protection act — this allows for enforcement by both the Washington attorney general's office and by private litigants. The private right of action makes the MHMDA unique in terms of state privacy laws. Given how aggressively plaintiffs have relied on the private

40 These states include: California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia.

41 See generally Cal. Civ. Code § 798.140(c) and (ae).

42 This includes, for example, the rights to know, correct, delete, and opt out of sales or "sharing."

43 The private right of action for customers aggrieved by an entity's violation is limited because customers can only use it if the entity does not fix its violation within a 30-day cure period after the customer reports the violation. See New York City Admin. Code § 22-1203.

44 Portland, OR., City Code § 34.10.050(A).

45 See generally Wash. Rev. Code § 19.373.005 et seq.

46 Unless the collection or sharing is required for a product or service specifically requested by a consumer.

right of action in BIPA and how unique the law's provisions are, it seems likely that the MHMDA will be a significant source of litigation activity.[47] Additionally, two other states (Nevada and Connecticut) have passed similar consumer health privacy laws (notably without a private right of action), indicating that this may be a new trend for state privacy laws.

04

THE CHALLENGES WITH REGULATING BIOMETRIC DATA

To date, the manner in which biometric data has been regulated in the United States — featuring an array of competing, and at times overlapping, frameworks articulated by federal and state legislatures and regulators — mirrors the approach taken in the broader privacy legal landscape. As is the case with biometric data, there is no single federal law governing data privacy generally. Instead, what has emerged is, in effect, a series of data type-specific federal laws (such as HIPAA for certain health information and the Gramm-Leach-Bliley Act for financial information), a canon of enforcement decisions by regulators like the FTC, and a growing collection of comprehensive privacy laws at the state level. Though efforts have been made over the years to develop a comprehensive privacy law at the national level, none have been successful, thus leaving the privacy patchwork in place.

In both contexts, the mishmash of competing legal frameworks has (and will continue to) hurt both businesses and consumers. A business setting out to process consumer data, whether biometric or not, in the current landscape will confront a daunting array of potentially applicable legal frameworks. This can be a particular challenge for smaller businesses that may lack the resources or legal expertise to develop and implement robust compliance programs. Faced with this, some companies may choose to conservatively tether themselves to the framework with the most stringent requirements. While this approach may shield a company from legal exposure, it may also result in resources being spent on unnecessary compliance efforts or stymied innovation. Other companies may simply ignore their privacy obligations altogether, which may save costs in the short term, but creates heightened liability for potentially serious enforcement and litigation exposure in the long run. Needless to say, neither of these extremes represents an ideal allocation of businesses' resources.

The biometric and general data privacy landscapes are confusing for consumers, as well. Given the multiplicity of potentially applicable laws, it can be challenging for consumers to discern what data protections they are entitled to and what data processing practices lie outside the scope of legally permissible conduct. This obscuring of what constitutes "good" versus "bad" data privacy practices can, in turn, have a warping effect on marketplace incentives. After all, if consumers are unable to determine whether a company's data practices are legal, they may continue to give their business to companies that fail to adequately safeguard consumer data, thus allowing those companies to continue to operate and thrive in the marketplace.

Finally, the patchwork approach arguably bestows too much power on jurisdictions that impose the most onerous requirements. For instance, in the general privacy sphere, California has emerged as the national trendsetter, enacting a statutory framework (based on the California Consumer Privacy Act and California Privacy Rights Act) that imposes relatively stringent requirements on businesses that process personal information,[48] developing regulations that further expand on those requirements,[49] and empowering regulators to enforce said requirements.[50] Given the size of the California market, most businesses above a certain revenue or information-processing threshold are effectively obligated to comply with California's privacy requirements. We have seen a similar effect in the biometric sphere, with companies nationwide working to conform their practices to align with the requirements of Illinois's BIPA, and thereby avoid being on the receiving end of that statute's severe statutory penalties. Whatever one thinks of the merits of the CCPA/CPRA and BIPA legal regimes, the effective outsourcing of national policymaking to individual states — representing only a subset of the national population and economy — surely cannot be the most effective way to develop these types of legal requirements.

47 The law went into effect on March 31, 2024 for regulated entities and will go into effect on June 30, 2024 for small businesses.

48 See Cal. Civ. Code § 1798.100 *et seq.*

49 See Cal. Code Regs. tit. 11, § 7000 *et seq*.

50 See e.g. California Privacy Protection Agency, *About CPPA*, https://cppa.ca.gov/about_us/ (last accessed Mar. 12, 2024); State of California Department of Justice, *Attorney General Bonta Announces Settlement with DoorDash, Investigation Finds Company Violated Multiple Consumer Privacy Laws* (Feb. 21, 2024), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-doordash-investigation-finds-company.

05
LOOKING AHEAD

The complexity of U.S. biometric privacy law is in many ways reflective of the broader U.S. privacy landscape—in both contexts, a complicated spectrum of federal and state legal frameworks present significant difficulties for regulators, companies, and individuals. Given the importance of biometric data privacy and current uncertainty in protections and compliance in the U.S., federal and state legislatures are expected to propose, debate, and potentially enact more laws that address biometric data privacy in the years to come, while regulators make continued efforts to exert their authority in the biometric privacy sphere. Indeed, the closing weeks of 2023 and opening months of 2024 have already seen such legislative and regulatory efforts emerge at the federal and state levels. The year kicked off with the FTC's enforcement action against Rite Aid, where Commissioner Bedoya opened his accompanying statement with a frank, "Biased face surveillance hurts people," signaling that regulators are keenly tuned into FRT developments.[51] Then New York legislators introduced the Biometric Privacy Act on both sides of the statehouse (A1362 and S4457), while Nebraska introduced the Biometric Autonomy Liberty Law (LB954). Only time will reveal whether the biometric privacy legal landscape ultimately converges on a unified, comprehensive approach, or instead continues to operate as a fragmented patchwork of legal frameworks.

"The complexity of U.S. biometric privacy law is in many ways reflective of the broader U.S. privacy landscape—in both contexts, a complicated spectrum of federal and state legal frameworks present significant difficulties for regulators, companies, and individuals

51 Statement of Commissioner Alvaro M. Bedoya, *supra* note 19.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL