Twin Inadequacies in the FTC's Recent Biometrics Policy Statement

John Burroughs[*]

In the spring of 2023, the FTC released a policy statement addressing biometric information and technologies using or purporting to use such information. The policy statement contains a remarkably broad definition of "biometric information" and describes a variety of business practices that could violate § 5 of the Federal Trade Commission Act by being either "deceptive" or "unfair." In spite of the policy statement's comprehensiveness, however, it has two substantial inadequacies. First, the policy statement's definition of "biometric information" is overly broad and will introduce unnecessary legal uncertainty for businesses by encompassing items not commonly thought of as "biometric information technologies" or not associated with the same risks. Second, the policy statement lacks any substantial analysis of when the potential risks to consumers associated with a business use of such technologies may be outweighed by benefits to consumers or competition, and the Federal Trade Commission Act requires such analysis before the FTC can declare any practice unlawful on account of being "unfair." The absence of this sort of cost-benefit analysis in the policy statement indicates that the FTC will likely focus on bringing "deception" charges, as the FTC has similarly done in the past when regulating data privacy. In turn, this focus on "deception" will likely result in a relatively passive and reactive regulatory regime centered around increased disclosure by businesses. Additional disclosures will not significantly benefit consumers, however, as information asymmetries make it difficult for them to weigh the risks associated with the business use of biometric information. Moreover, potential mismanagement and misuse of biometric information technologies can put consumers at risk of experiencing irreparable harm, which necessitates a proactive regulatory regime that can prevent harms before they occur. To address these twin inadequacies, the FTC should first narrow the definition to avoid covering information that is not commonly considered biometric. Then, the FTC should explicitly perform the cost-benefit analysis required to determine when the listed considerations which suggest that a business practice is "unfair" may render that practice unlawful, which will allow the FTC to focus more on "unfairness" charges and thereby enable more proactive regulation of this field. Revising the policy statement in this manner will allow it to strike the right balance between the commercial and noncommercial interests of consumers and businesses alike.

[*] J.D. Candidate 2025, University of Chicago Law School. Many thanks to Professor Josh Avratin for his invaluable feedback and guidance, and to my family for their constant support. Thank you as well to the *University of Chicago Business Law Review* editorial staff.

I. INTRODUCTION

On May 18, 2023, the Federal Trade Commission (FTC) released a new policy statement—the Policy Statement of the Federal Trade Commission on Biometric Information and § 5 of the Federal Trade Commission Act (the "policy statement")—addressing biometric information and technologies using or purporting to use such information.[1] Biometric information technologies have grown increasingly widespread in recent decades, and the biometrics market surrounding them is now valued in the billions.[2] In the absence of comprehensive federal law addressing the use of such information and technologies, the FTC's policy

[1] *See* Alison Frankel, *FTC Gives Businesses More Reasons to Worry About Biometric Privacy*, REUTERS (May 19, 2023), https://perma.cc/U3U3-SE8U.

[2] *See* Ariel Latzer, *Complying with New and Existing Biometric Data Privacy Laws*, 16 J. BUS. ENTREPRENEURSHIP & L. 201, 202 (2023).

statement currently represents the most extensive federal regulation in this area.[3]

The policy statement provides a remarkably broad definition of "biometric information," stating that the term "refers to data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body."[4] This is said to cover records capturing a variety of physical identifiers (such as facial features and fingerprints) as well as behavioral ones (such as gait or typing pattern),[5] with a provided example being a photograph of someone's face.[6]

"Biometric information technology," which the policy statement says has sometimes "been used to refer specifically to technologies that are used to identify individuals,"[7] is consequently defined to encompass "the broader category of all technologies that use or purport to use biometric information for any purpose."[8] The policy statement notes the various risks presented by biometric information and biometric information technologies before describing a variety of business practices involving them that could violate § 5 of the Federal Trade Commission Act by being either "deceptive" or "unfair."[9] This non-exhaustive list includes "[d]eceptive statements about the collection and use of biometric information,"[10] "[e]ngaging in surreptitious and unexpected collection or use of biometric information,"[11] "[f]ailing to evaluate the practices and capabilities of third parties . . . who will be given access to consumers' biometric information or will be charged with operating biometric information technologies,"[12] and more.

In its current form, the policy statement contains two inadequacies which will inhibit the effectiveness of FTC regulation in this field. First, its extremely broad definition of "biometric information" and "biometric information technologies" will introduce

---

3 *See, e.g.*, Alina Big, *Automatic Deletion of Biometric Data in Financial Institutions*, 45 SETON HALL LEGIS. J. 151, 155 (2021).

4 U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 1 (2023).

5 *Id.*

6 *Id.*

7 *Id.* at 1 n.2.

8 *Id.*

9 *See id.* at 5.

10 *Id.* at 7.

11 *Id.* at 10–11.

12 *Id.* at 11.

unnecessary legal uncertainty regarding the scope of the FTC's regulation. By encompassing "all technologies that use or purport to use biometric information for any purpose,"[13] the policy statement applies to essentially any technology that records any physical or behavioral characteristic of a person, no matter how commonplace or mundane (such as photographs, audio recordings, and perhaps even written descriptions of physical features). Moreover, the definition does not make any distinction between "biometric information technologies" that serve fundamentally different purposes despite all nominally having the potential use of identifying individuals (for example, X-ray scans used in a medical context, security devices like security cameras, or verification technologies like facial recognition). The definition as it now stands will thus confuse businesses by encompassing a variety of items not commonly thought of as "biometric information technologies" and not associated with the same uses or risks.

Second, the Federal Trade Commission Act states that the FTC has "no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[14] While the policy statement details the ways in which the mismanagement or misuse of biometric information technologies is likely to cause substantial injury to consumers and also describes how such harms may not be reasonably avoidable by consumers, it does not contain any analysis of when benefits to consumers or competition may outweigh these factors. The absence of the sort of cost-benefit analysis required by the statute strongly suggests that the FTC will largely focus on the listed "deceptive" business practices, which is in line with the FTC's past practices in the field of data privacy regulation. Businesses can relatively easily avoid "deception" charges by providing more disclosure, but increased disclosure will be of little benefit to consumers, as information asymmetries make it difficult for them to estimate the risks associated with providing their biometric information. Moreover, the harms that can befall consumers due to these technologies—such as data breaches leading to security vulnerabilities—are nearly impossible to rectify after the

---

[13] *Id.* at 1 n.2.

[14] 15 U.S.C. § 45(n).

fact, which necessitates a more proactive regulatory regime that stops harms before they occur.

To address these issues, the FTC should narrow the definition in the policy statement to avoid encompassing technologies that are not commonly considered biometric or associated with the same risks and explicitly lay out the cost-benefit analysis which will allow it to declare business practices unlawful based on the listed "unfairness" considerations, thereby enabling more proactive regulation. Doing so will help the FTC strike the proper balance between the interests of consumers and businesses and allow both to enjoy the remarkable economic benefits biometric information technologies offer.

II. BIOMETRIC INFORMATION TECHNOLOGIES

A. Defining Biometrics

Putting aside any specific statutory or regulatory definitions, biometric information generally encompasses the distinctive bodily traits of an individual, and can be divided into two categories.[15] First and most obviously, biometric information covers one's physical characteristics, such as fingerprints.[16] Second and less intuitively, biometric information can also cover behavioral patterns like gait or typing speed.[17] Biometric information technologies thus constitute technologies that gather, record, and analyze biometric information.[18] Examples of such technologies include facial recognition software and retinal scanning.[19]

Biometric information technologies thus allow for easy identification and verification of individuals.[20] When using such a technology, the specific biometric trait which will later be used for identification or verification must first be provided and stored in

---

[15] Chloe Stepney, *Actual Harm Means It Is Too Late: How* Rosenbach v. Six Flags *Demonstrates Effective Biometric Information Privacy Law*, 40 LOY. L.A. ENT. L. REV. 51, 53 (2019).

[16] Cristina Del Rosso, *Access Granted: An Examination of Employee Biometric Privacy Laws and a Recommendation for Future Employee Data Collection*, 18 J.L. ECON. & POL'Y 24, 26 (2023).

[17] *Id.*

[18] *See* Anna L. Metzger, *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).

[19] Daveante Jones, *Protecting Biometric Information in Arkansas*, 69 ARK. L. REV. 117, 118–119 (2016).

[20] Del Rosso, *supra* note 16, at 26.

order to be useful.[21] Once this is done, an individual can later present the proper biometric characteristic to the technology and allow it to be matched with the previously provided characteristic.[22] If the technology is used for verification, it will match the presented trait with the recorded one in order to confirm the individual's identity.[23] If the technology is used for identification, it will review a database of provided characteristics to match the presented trait with one of them and thereby determine the identity of the individual possessing the presented trait.[24] These two uses are sometimes called "one-to-one" matching and "one-to-many" matching, respectively.[25] Biometrics can also facilitate classification—in essence a subset of identification—where a given trait allows a technology to categorize an individual by estimating other characteristics such as race, age, or gender.[26]

While biometric information technology can in theory be based upon any physiological or behavioral characteristic, there are certain desired features which determine what biometric information is considered valuable. Characteristics which are defined by universality, uniqueness, permanence, and other features which increase the reliability and ease of identification and verification are particularly well-suited for use in biometric information technologies.[27]

B. Commercial Value

Given the above information, it is not surprising that biometric information and biometric information technologies have become sources of immense commercial value in recent decades.[28] The use of such technologies can benefit both consumers and businesses alike. From the perspective of consumers, traditional methods of identification or verification such as passwords or identifying documents can be either inconvenient (if forgotten or

---

21 Metzger, *supra* note 18, at 1053.

22 Elizabeth M. Walker, *Biometric Boom: How the Private Sector Commodifies Human Characteristics*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 831, 837 (2015).

23 *Id.*

24 *Id.*

25 *Id.*

26 *See, e.g.*, Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 621 (2019).

27 *See* Jones, *supra* note 19, at 119–20.

28 *See* Latzer, *supra* note 2, at 202.

lost) or insecure (if guessed, stolen, or forged).[29] In contrast, biometric information generally cannot be lost and is much more difficult to replicate than a password or document.[30] Thus, biometric information technologies provide consumers with a system of identification or verification that is simultaneously more convenient and more secure. As a result of these advantages, biometric information technologies have become increasingly ubiquitous in daily life, with consumers using them for both menial tasks (like unlocking one's phone) and substantial activities (like authenticating financial transactions).[31]

For businesses, biometric information and biometric information technologies can have their commercial value based on several factors. For one, businesses which utilize biometric information technologies can offer more convenience and security for their customers and can thereby gain a competitive advantage over their business rivals. The efficacy of such technologies can also lower a business's operational costs.[32] From an internal perspective, businesses can use these technologies for security purposes or as a means of monitoring employees.[33] Finally, the external sale and exchange of biometric information can be a source of value. Businesses who themselves have no use for a collected biometric identifier may opt to sell that biometric information to other businesses which desire it for their own commercial purposes, such as consumer behavioral analysis.[34] Elias Wright describes this practice and provides an example:

> Facial recognition, when used as a unique persistent identifier in a data management system, enables organizations to structure previously unstructured video data, associating an identity with other raw data such as previous purchases, emotional response, age, gender, and in-store movement patterns, and increasing the value of the customer profile. When analyzing consumer decision-making, consumer engagement that does not result in a conversion or purchase may be as significant as those transactions that are recorded in financial data.

---

29 Metzger, *supra* note 18, at 1060.

30 *Id.*

31 *See* Stepney, *supra* note 15, at 54.

32 *Id.* at 59.

33 Metzger, *supra* note 18, at 1060.

34 *See* Wright, *supra* note 26, at 631–32.

> Biometric identification techniques, when shared across data collectors, then dramatically expand the sources from which consumer data may be drawn, increasing the accuracy and invasiveness of aggregate profile creation. The effects of biometric data's utility—identifying specific individuals—compound privacy risks from data aggregation. Consumer profiles assembled using biometrics are more valuable to data brokers as they provide greater profile accuracy. In a marketplace where aggregate consumer data often contains incorrect and erroneous information, increasing the accuracy of information is highly lucrative for data brokers. More accurate data allows for higher confidence in insights, which allows for a competitive advantage to the data's users in predicting consumer's actions.[35]

As this example demonstrates, business use of biometric information and biometric information technologies thus exposes consumers to accompanying risks.

C. Risks

The risks of biometric information technologies can be roughly grouped into security risks and privacy risks. These two groupings largely correspond to the potential uses of these technologies, as security risks are usually tied to the verification aspect of biometric information technologies, whereas privacy risks are often associated with the use of these technologies for identification.

Security risks result from the unchangeable nature of most biometric information. While the physical or behavioral quality of this information usually makes it more secure than other forms of data due to being difficult to forge, its permanent nature renders it uniquely vulnerable to data breaches.[36] Unlike traditional verification methods like passwords or documents, one cannot change or replace biometric information once it has been compromised.[37] The same permanence that makes this information valuable for verification thus renders it almost worthless for

---

[35] *Id.* at 632–33 (footnotes omitted).

[36] Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769, 774 (2018).

[37] *Id.*

verification if there is a data breach, which harms the consumer by depriving them of the economic benefits biometric information technologies can offer. This is, of course, in addition to the obvious fact that compromised biometric information can be used to access anything protected by that form of biometric verification (such as personal records or financial accounts), which clearly harms consumers. Biometric information technologies therefore render consumers uniquely exposed to the risks of data breaches, which are growing increasingly common each year (with more than 783 hacks affecting over 85.61 million records occurring between 2005 and 2014).[38]

Privacy risks are a natural consequence of the collection of large amounts of biometric information for identification purposes. A high degree of collection facilitates intrusive surveillance and thus conflicts with the privacy interests of consumers.[39] Indeed, this risk is where the interests of businesses most directly conflict with those of consumers. Businesses may desire to use biometrics to track individuals and record information about habits and preferences in order to form a more comprehensive—and thus more useful—customer profile.[40] This can benefit consumers by providing them with more personalized ads, products, and services. Despite this, a study by the Consumer Technology Association found that consumers were less comfortable with this sort of surveillance-based personalization than merely using biometrics for verification,[41] and a separate 2018 study by the Brookings Institution revealed that "50% of participants found the use of facial recognition in retail settings to prevent theft unfavorable, with 42% of those surveyed stating that facial recognition was an invasion of personal privacy."[42] In addition to these concerns, biometric information technologies may also result in discrimination against protected classes—whether intentional or unintentional—due to their ability to classify individuals into groups such as race, age, or gender.[43] These sorts of classifications result in further privacy risks due to potentially revealing sensitive and

---

38 Big, *supra* note 3, at 161.

39 *See* Wright, *supra* note 26, at 626.

40 *Id.* at 630–33.

41 *See id.* at 626.

42 *Id.*

43 *See, e.g.*, Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 351 (2014); Wright, *supra* note 26, at 621.

private information "such as pregnancy status, sexual orientation, political and religious views, or drug use."[44]

III. CURRENT LAW

Despite the broad risks associated with biometric information technologies and their increasing commercial use by businesses, there exists no comprehensive federal law regarding these technologies or their commercial use.[45] In the absence of federal regulation, several states have passed legislation regulating the use of biometric information technologies and the collection of biometric information more broadly. In particular, while a handful of other states have passed legislation governing biometric information in limited circumstances (such as for K-12 students) or have laws regulating personal data that partially touch on some aspects of biometric information,[46] only Illinois, Texas, and Washington have enacted comprehensive laws concerning biometrics.[47]

A. State Laws

The three current state laws that comprehensively address biometric information technologies and their commercial use by businesses present contrasting ways of regulating this field. Illinois has adopted a comparatively strict regime that places much more onerous requirements on businesses seeking to collect or use biometric information, but in turn it provides the strongest protections for consumers out of all the existing state laws. In contrast, Texas and Washington both contain relatively more lax regulations, though this comes at the cost of potentially leaving consumers more exposed to risk.

Regardless of which approach along this spectrum of strictness one believes is ultimately preferable, there are some features shared by state laws on both sides of the continuum. The most notable commonalities are those which work to curtail the scope

---

44 Hirsch, *supra* note 43, at 346 (footnotes omitted).

45 *See, e.g.*, Big, *supra* note 3, at 155.

46 *See* Blake Benson, *Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy*, 19 N.C. J.L. & TECH. 161, 171 (2018); Del Rosso, *supra* note 16, at 42–43; Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA HIGH TECH. L.J. 39, 62–85 (2021).

47 *See* Eliza Simons, *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, 1112 (2021).

of the state laws, and strikingly this is often accomplished through limitations on the definition of "biometric information." For example, both Illinois and Texas limit their statutory definitions of "biometric information" to a specific, limited universe of information, rather than relying upon a more general definition encompassing the distinctive bodily traits of an individual. Illinois and Washington also explicitly lay out a variety of types of information that do not count as "biometric information" for the purposes of their statutes, including everyday items such as photographs. Finally, both Illinois and Washington exclude some forms of information from their statutory definitions on the basis of the context in which it is gathered rather than the type of information itself. Both states exclude a variety of healthcare-related information, and Washington also contains exclusions for information gathered for security purposes. The healthcare exclusions in particular seem reasonable, given the extent to which healthcare information is already subject to other regulatory regimes (and indeed, both Illinois and Washington explicitly exclude "information collected, used, or stored for health care [sic] treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996").[48]

Given how variable the three existing state laws in this area are in terms of strictness, it is remarkable that they are in agreement when it comes to carefully curtailing their scope through how they define "biometric information." This precise policing of the boundaries of what is and is not covered suggests an attention to the risks of unduly regulating technologies not usually thought of as biometric or not associated with the same risks. In particular, these precise definitions likely lower business uncertainty and assist in efforts to comply with the law while also making sure to not unduly burden businesses or interfere with regulatory regimes addressing different fields. Moreover, this unanimity regarding limited definitions contrasts sharply with the FTC's recent policy statement, which contains no such definitional limitations on its scope and thus breaks with the approach adopted by the states.

i. Illinois

Illinois became the first state to enact comprehensive biometrics legislation when it passed the Biometric Information Privacy

[48] 740 ILL. COMP. STAT. 14/10; 74 WASH. REV. CODE § 19.375.010(1).

Act (BIPA) in 2008.[49] The BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual,"[50] with "biometric identifier" being defined to exclusively mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[51] The BIPA further states, however, that some categories of physical or behavioral identifying information are not considered to be "biometric identifier[s]," as the term "do[es] not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[52] The BIPA also excludes from its definition a variety of information gathered in healthcare contexts, including "information captured from a patient in a health care [sic] setting"[53] and "an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening."[54]

When it comes to the collection and use of biometric information, the BIPA requires that private entities receive a written release before obtaining any biometric information,[55] and further provide written notification to any individual whose biometric information is collected or stored, with such notification including "purpose and length of use."[56] Additionally, the BIPA requires private entities to develop and make public a written policy governing retention and destruction of biometric information:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the

---

49 Benson, *supra* note 46, at 171.

50 740 ILL. COMP. STAT. 14/10.

51 *Id.*

52 *Id.*

53 *Id.*

54 *Id.*

55 Hannah Harper, *Your Body, Your Data, But Not Your Right of Action: Seeking Balance in Federal Biometric Privacy Legislation*, 8 NAT'L SEC. L.J. 86, 97 (2021).

56 *Id.* at 96.

> initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.[57]

Two other especially notable features of the BIPA are that it completely prohibits the commercial sale of biometric information, [58] and that it creates a private right of action for violations of the statute,[59] which Illinois courts have interpreted to allow suits for purely statutory harm.[60]

Given the characteristics outlined above, the BIPA places the heaviest burden on businesses out of any of the existing state laws.[61] Despite this, the BIPA also contains some key limitations which curtail the scope of its relatively onerous requirements. Crucially, these limitations are found in how the BIPA defines what counts as a "biometric identifier." This term is limited to a specific universe of listed items ("a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"),[62] and for good measure a variety of commonplace descriptors such as "photographs, . . . tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color"[63] are explicitly excluded from the definition. Moreover, in addition to limiting the definition to certain types of information, the BIPA also excludes information gathered for specific purposes or in certain contexts when it excludes "information captured from a patient in a health care [sic] setting"[64] and any "image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening."[65] The BIPA thus exemplifies an approach that strictly regulates business use of biometric information technologies while also carefully delineating what is and is not considered to be "biometric information," and thereby avoids overextending the application of its strict regulations.

---

57 740 ILL. COMP. STAT. 14/15(a).

58 *Id.* 14/15(c).

59 740 ILL. COMP. STAT. 14/20; Harper, *supra* note 55, at 97.

60 *See* Savannah G. Stewart, *Privacy—When Is an Individual's Biometric Data Protected?*, 43 AM. J. TRIAL ADVOC. 269, 272–73 (2019).

61 *See, e.g.*, Benson, *supra* note 46, at 171–79.

62 740 ILL. COMP. STAT. 14/10.

63 *Id.*

64 *Id.*

65 *Id.*

ii. Texas

In 2009, Texas passed the Capture or Use of Biometric Identifiers Act (CUBI) and thus became the second state to enact comprehensive biometrics legislation.[66] The CUBI specifically defines "biometric identifier" to exclusively cover "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[67] The statute subjects companies to a variety of disclosure, security, and retention limits.[68] In particular, the CUBI prohibits the collection of such biometric identifiers for commercial purposes unless the individual possessing the information is first informed and gives consent.[69] Additionally, any person who possesses a biometric identifier collected for commercial purposes "shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires,"[70] except when retention for a longer period is otherwise required by law. Finally, there is no private right of action under the CUBI (unlike the Illinois BIPA), so the Attorney General must be the one to bring actions for violations of the law and recover civil penalties.[71]

While the CUBI places comparatively less strict regulations on the business use of biometric information technologies than the Illinois BIPA, it is thus remarkable that the definition of "biometric identifier" provided in the CUBI (exclusively meaning "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry")[72] is almost entirely identical to the definition of "biometric identifier" provided in the BIPA (exclusively covering "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry")[73] despite these differences. This crucial similarity suggests that definitionally limiting the regulated "biometric information technologies" to a specific universe of listed items is a worthwhile approach regardless of the ultimate level of strictness desired for the regulations.

---

66 *See* Wright, *supra* note 26, at 642.

67 11 TEX. BUS. & COM. CODE § 503.001(a).

68 Lisa P. Angeles, *Untag Me: Why Federal Judges Are Broadly Construing Illinois's Biometric Privacy Law*, 42 CARDOZO L. REV. 349, 359 (2020).

69 *Id.*

70 11 TEX. BUS. & COM. CODE § 503.001(c)(3).

71 Angeles, *supra* note 68, at 359.

72 11 TEX. BUS. & COM. CODE § 503.001(a).

73 740 ILL. COMP. STAT. 14/10.

iii. Washington

The Washington Biometric Privacy Act (WBPA) enacted in 2017 is the most recent comprehensive state biometrics law.[74] The WBPA defines "biometric identifier[s]" as encompassing "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 [sic] used to identify a specific individual."[75] Similar to the Illinois BIPA, the WBPA contains specific exclusions for information gathered in certain contexts, as the WBPA specifics that "biometric identifier" does not cover "a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care [sic] treatment, payment, or operations under the federal health insurance portability and accountability act of 1996 [sic]."[76] The WBPA also defines "biometric system[s]" as "automated identification system[s] capable of capturing, processing, and storing a biometric identifier, comparing the biometric identifier to one or more references, and matching the biometric identifier to a specific individual."[77]

Instead of regulating all collection of biometric information, the WBPA only regulates commercial use. It prohibits recording a biometric identifier in any database for a commercial purpose "without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[78] The WBPA further states that any notice must provide disclosure through a procedure designed to be available to any affected individual and states that the precise notice and type of consent required will depend on context.[79] However, there are several exceptions to these notice requirements, most notably if the collection of biometric information is for a "security purpose," which "include[s] preventing shoplifting, other misappropriation or theft, and other purposes in furtherance of protecting security."[80] Like the Texas CUBI and unlike the Illinois BIPA, the WBPA does not provide a private cause of action.[81] The

---

74 *See* Michelle J. Anderson & Jim Halpert, *Washington Become the Third State with a Biometric Privacy Law: Five Key Differences*, 1 RAIL 41 (2018).

75 74 WASH. REV. CODE § 19.375.010(1).

76 *Id.* § 19.375.010(1).

77 *Id.* § 19.375.010(2).

78 *Id.* § 19.375.020(1).

79 *See id.* § 19.375.020(2).

80 Anderson & Halpert, *supra* note 74, at 44.

81 *Id.* at 44–45.

WBPA is thus a more narrowly curtailed regulation in both its scope and its effect.[82]

The WBPA is perhaps the least onerous of all the existing state laws regulating the business use of biometric information technologies. In spite of this, however, both it and the Illinois BIPA explicitly exclude from their statutory definitions certain technologies that are not usually thought of as biometric or not associated with the same uses or risks, such as everyday items like photographs. Moreover, both the WBPA and the BIPA exclude some types of information related to healthcare from their statutory definitions based on the context in which it is collected rather than the form of information itself, and in particular both explicitly exclude "information collected, used, or stored for health care [sic] treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996."[83] The fact that these definitional limitations are shared by both the most and the least strict state laws in this area speaks to their usefulness in preventing regulations addressing the business use of biometric information technologies from being overextended or interfering with regulatory regimes addressing different areas.

B. Lack of Federal Law

As previously stated, there currently exists no comprehensive federal law regulating biometric information or biometric information technologies. Moreover, as demonstrated above, the vast majority of states do not contain substantive consumer protections for biometric information technologies. In fact, the existence of the strongly pro-consumer BIPA has discouraged other states from passing similar biometric information laws, given the frequent litigation in Illinois and subsequent lobbying in other states from interested companies hoping to avoid similar litigation in other jurisdictions.[84] As a result, though at least eleven other states have attempted to pass comprehensive state biometrics laws, none of these attempts have succeeded.[85]

With state efforts to increase consumer protections stalled, the stage is set for federal regulation in this area. Biometric

---

[82] *Id.* at 41.

[83] 740 ILL. COMP. STAT. 14/10; 74 WASH. REV. CODE § 19.375.010(1).

[84] Benson, *supra* note 46, at 180.

[85] *See* Gabrielle Neace, *Biometric Privacy: Blending Employment Law with the Growth of Technology*, 53 UIC L. REV. 73, 91 (2019).

information technologies are only becoming more commonplace, and in turn the serious risks associated with them are becoming more apparent.[86] The few state laws that do exist are inconsistent (as seen above), so federal law in this area could resolve business uncertainty by providing a uniform standard.[87] Moreover, the vast majority of technology companies gathering this information and developing these technologies operate throughout the country and across state lines, making federal intervention even more appropriate.[88] Based on these considerations, commentators are broadly in agreement that federal regulation in this area would be ideal.[89] In particular, the prominent privacy risks would seem to point towards regulation of biometric information technologies by the FTC, given the informal role it has adopted as the primary United States privacy regulator.[90]

Considering the wide-ranging potential benefits of biometric information technology to consumers and businesses on one hand, and the risks to consumers outlined above on the other, federal regulation of biometrics should seek to mitigate the potential risks while also enabling consumers and businesses to take advantage of the economic benefits that these technologies have to offer. Federal law should thus seek to lessen legal uncertainty by providing clear rules and suggested practices for businesses to follow, which would allow them to ensure compliance while also pursuing continued development and innovation in this field.[91] Moreover, as some of the harms associated with these technologies—such as data breaches leading to security vulnerabilities—are nearly impossible to rectify after the fact, federal regulation should aim to proactively protect consumers from these harms before they occur. [92] Hewing closely to these several goals will allow federal regulation to strike the ideal balance between the commercial and noncommercial interests of both consumers and businesses.

---

86 Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 637–39 (2018).

87 *Id.* at 638–39.

88 *See* Pope, *supra* note 36, at 797.

89 *See id.*; *see also* Zimmerman, *supra* note 86, at 638–39.

90 *See* Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 648 (2021).

91 *See* Pope, *supra* note 36, at 797–98.

92 *See id.* at 771–74.

IV. RECENT FTC POLICY STATEMENT

On May 18, 2023, the FTC released its recent policy statement targeting biometric information and biometric information technologies.[93] The policy statement begins with a definition of these two terms before then calling attention to the various risks they may pose to consumers.[94] The policy statement concludes with a non-exhaustive listing of some business practices that could violate § 5 of the Federal Trade Commission Act by being either "deceptive" or "unfair."[95]

Of course, just as notable as what is included is what is not included in the policy statement. The policy statement does not include any limitations on its definitions of "biometric information" and "biometric information technologies" resembling those found in state laws addressing this area. Unlike the Illinois BIPA and the Texas CUBI, it does not limit its definition of "biometric information" to a set universe of listed items. The policy statement also does not contain exclusions for information collected in certain contexts, or for certain types of technologies not usually considered to be biometric or not associated with the same uses or risks, unlike the BIPA or the WBPA. The lack of these features suggests that the policy statement is at risk of being overextended, perhaps even to the point of conflicting with federal regulatory regimes addressing different areas such as healthcare. This in turn will increase legal confusion for businesses and make it more difficult for them to comply with the law.

The policy statement also lacks even a preliminary cost-benefit analysis of when the potential risks associated with a business use of biometric information may be outweighed by benefits to consumers or competition. Such a determination would need to be made before the FTC could declare any practice unlawful due to being "unfair," as the Federal Trade Commission Act provides that the FTC cannot do so "unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[96] By

---

[93] *See* Alison Frankel, *FTC Gives Businesses More Reasons to Worry About Biometric Privacy*, REUTERS (May 19, 2023), https://perma.cc/U3U3-SE8U.

[94] U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 1–5 (2023).

[95] *Id.* at 5–12.

[96] 15 U.S.C. § 45(n).

itself, this would make it more difficult for businesses to determine exactly what business practices are covered and how businesses can comply with the requirements of § 5. Furthermore, the absence of any attempt at such an analysis strongly suggests that the FTC will largely focus on the listed "deceptive" business practices, similar to how the FTC has treated regulation of data privacy.[97] This focus on "deceptive" practices will itself likely only lead to increased disclosures by businesses, which ultimately will be of little benefit to consumers.

A. Scope

The policy statement advances an extremely broad definition of "biometric information," stating that the term "refers to data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body."[98] As used by the FTC, the term "includes, but is not limited to, depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern),"[99] as well as "data derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data had been derived."[100] "Biometric information technologies" is in turn said to encompass not only "technologies that are used to identify individuals,"[101] but also "the broader category of all technologies that use or purport to use biometric information for any purpose."[102]

Strikingly, nowhere in these definitions are exclusions for certain types of information as are commonly found in state laws. The policy statement's definition of "biometric information" broadly encompasses the distinctive bodily or behavioral traits of an individual, and the list of examples provided explicitly does not capture the full universe of covered technologies. Moreover, the policy statement does not provide any example of a type of

---

97 Cobun Keegan & Calli Schroeder, *Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms*, 15 J.L. ECON. & POL'Y 19, 28 (2019).

98 U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 1 (2023).

99 *Id.*

100 *Id.*

101 *Id.* at 1 n.2.

102 *Id.*

information that would not be considered biometric, which could be helpful in clarifying the true extent of the definition. The definition also does not contain any exclusions for information collected in different contexts, such as for healthcare or security purposes. Perhaps most remarkably, the policy statement outright states that a photograph of someone's face—one of the items explicitly excluded in the Illinois BIPA and the WBPA—is an example of "biometric information."[103]

B. Recognized Risks

The policy statement then lays out multiple developments in this field which have exposed consumers to risks and necessitated the FTC's intervention. Some of these are simply developments in biometric information technologies and the market for them, such as the growing commercial prevalence of these technologies and their vastly increased efficacy.[104] Others, however, relate more directly to the security and privacy risks associated with these technologies. For example, the policy statement flags the security risk of collected data being accessed by bad actors for use in fraud.[105] The policy statement also identifies privacy risks by highlighting the risk of data collection revealing sensitive personal information about consumers (such as, "for example, [revealing] that they have accessed particular types of healthcare, attended religious services, or attended political or union meetings")[106] and the danger of harmful or unlawful discriminatory outcomes resulting from the use of biometric information technologies (for example, by giving false positives or false negatives due to the technology being less effective for a given race, gender, or other protected class).[107] The policy statement draws extensive attention to this last issue in particular:

> [R]esearch published by the National Institute of Standards and Technology (NIST) found that many facial recognition algorithms produce significantly more false positive "matches" for images of West and East African and East Asian faces than for images of Eastern European faces. The research also found rates of false

[103] *Id.* at 1.
[104] *Id.* at 2.
[105] *Id.* at 3–4.
[106] *Id.* at 4.
[107] *Id.* at 4–5.

> positives to be higher in women than men, and in the elderly and children compared to middle-aged adults. Demographic differentials may be even more pronounced when analyzed intersectionally (e.g., when comparing light-skinned males to dark-skinned females, rather than simply males to females and light-skinned subjects to dark-skinned subjects). Similarly, some biometric information technologies, such as those that process facial images or voice recordings, may be particularly prone to error when the subject of the analysis is a person with a disability. In light of this potential for bias, such technologies can lead or contribute to harmful or unlawful discrimination. This is particularly concerning when such technologies are used to determine whether consumers can receive important benefits and opportunities or are subject to penalties or less desirable outcomes. For example, if biometric information technologies are used to provide access to financial accounts, a false negative may result in the consumer being denied access to their own account, whereas a false positive may result in an identity thief gaining access to the account. If biometric information technologies are used for security surveillance, false positives may result in individuals being falsely accused of crimes, subjected to searches or questioning, or denied access to physical premises.[108]

Finally, the policy statement emphasizes the difficulties faced by consumers in avoiding the above risks and unintended consequences as another justification for intervention in this area.[109]

C. Scrutinized Practices

In light of these developments, the policy statement lists a variety of practices that the FTC will scrutinize when determining whether a company's use of biometric information or biometric information technologies is "deceptive" or "unfair," which would violate § 5 of the Federal Trade Commission Act.[110] While

---

[108] *Id.* (footnotes omitted).

[109] *Id.* at 4.

[110] *Id.* at 5–12; 15 U.S.C. § 45(a)(1).

this listing is explicitly non-exhaustive,[111] it nevertheless provides insight as to the general kind of practices the FTC will devote its attention to when regulating biometrics.

i. "Deception"

First, the policy statement sets out two examples of business practices that would qualify as "deceptive" under § 5. The first is "[f]alse or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information."[112] The policy statement indicates that the FTC intends to carefully examine the marketing surrounding these technologies to ensure that businesses are not making "false or unsubstantiated" claims about the technologies' accuracy, freedom from bias, or ability to deliver particular results.[113] Moreover, the policy statement says that "[c]laims of validity or accuracy are deceptive if they are true only for certain populations and if such limitations are not clearly stated."[114] The second listed practice is, rather reasonably, "[d]eceptive statements about the collection and use of biometric information."[115] This includes making false statements about the extent to which biometric information is collected and used, as well as telling "half-truths" by disclosing some purposes for which the information will be used without disclosing others.[116]

ii. "Unfairness"

The policy statement then turns to business practices that could constitute "unfairness" under § 5. Generally, a practice is "unfair" for the purposes of § 5 "if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[117] Given the risks recognized by the policy statement that are outlined above, it states that the collection and use of biometric information can lead to

---

111 U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 5 (2023).

112 *Id.* at 6.

113 *Id.*

114 *Id.*

115 *Id.* at 7.

116 *Id.*

117 *Id.*

significant risks for consumers.[118] The policy statement further stresses that potential harms are not reasonably avoidable whenever the collection and use "is not clearly and conspicuously disclosed or if access to essential goods and services is conditioned on providing the information."[119] Ultimately, businesses should enact reasonable data security measures to protect collected or retained biometric information from being compromised by both external intruders and internal unauthorized employees or affiliated parties.[120] Furthermore, the policy statement notes that determining whether any particular business use of biometric information or biometric information technologies violates § 5 requires "a holistic assessment of the business's relevant practices,"[121] and that the FTC will draw on its past work in areas such as privacy and data security when making such assessments.[122] Moreover, the policy statement says that business practices may run afoul of § 5 if the resulting risks to consumers outweigh the potential business benefits.[123] Such practices may thus amount to unfairness, as "if more accurate, less risky alternatives are available, using a technology that is proven to have high error rates may present unjustifiable risk to consumers, even if the technology is more convenient, more efficient, or more profitable for the business considering implementing the technology."[124]

With these general foundations in place, the policy statement proceeds to describe factors that would be considered when determining whether a business practice constitutes "unfairness" under § 5.[125] Most of these listed factors involve omissions or failures to comply which invoke both the security and privacy risks associated with biometric information technologies. For example, "[f]ailing to evaluate the practices and capabilities of third parties . . . who will be given access to consumers' biometric information or will be charged with operating biometric information technologies"[126] could potentially expose consumers to both security and privacy risks. This is also the case with "[f]ailing to provide appropriate training for employees and contractors whose job

---

118 *Id.*
119 *Id.*
120 *Id.* at 8–9.
121 *Id.* at 9.
122 *Id.*
123 *Id.*
124 *Id.*
125 *Id.* at 9–12.
126 *Id.* at 11.

duties involve interacting with biometric information or technologies that use such information"[127] and "[f]ailing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses in connection with biometric information."[128] Likewise, "[f]ailing to assess foreseeable harms to consumers before collecting biometric information"[129] and "[f]ailing to promptly address known or foreseeable risks"[130] both invoke security and privacy risks, and potentially even classification concerns if there are disparate impacts affecting members of protected classes. Finally, one listed potential factor only involves practices which create privacy risks for consumers. This is the case with "[e]ngaging in surreptitious and unexpected collection or use of biometric information,"[131] which covers practices which "expose[] the consumer to risks such as stalking, exposure to stigma, reputational harm, or extreme emotional distress"[132] (which would be considered "unfair in and of itself"),[133] as well as failure to clearly and conspicuously disclose the collection and use of biometric information to affected individuals (thereby automatically rendering these practices unavoidable).[134]

V. ANALYSIS

There are two inadequacies which will hinder the effectiveness of the policy statement. First, the extremely broad, general definition of "biometric information" will introduce unnecessary legal uncertainty regarding the scope of the FTC's regulation. The definition as it now stands contains no exclusions for technologies not usually thought of as biometric or not associated with the same uses or risks and no exceptions for information collected in certain contexts, which will exacerbate the legal confusion for businesses. The fact that the policy statement lacks any explicit limitations on its extremely broad definition is especially notable given that even the strictest existing state laws regulating biometrics implement some definitional limitations. The adoption of at least some of these limitations present in state laws would

---

127 *Id.*
128 *Id.* at 12 (footnotes omitted).
129 *Id.* at 9–10.
130 *Id.* at 10.
131 *Id.* at 10–11.
132 *Id.*
133 *Id.* at 10.
134 *Id.* at 11.

likely significantly reduce the current ambiguity surrounding the scope of the policy statement and thereby prevent undue burdening of businesses.

Second, while the policy statement analyzes when certain business practices may cause substantial injury to consumers and when these injuries may not be considered reasonably avoidable, it lacks even a preliminary analysis of when possible risks associated with a business use of biometric information technologies may be outweighed by benefits to consumers or competition. It thus does not address the final statutory requirement laid out in the Federal Trade Commission Act that must be met before the FTC may declare a business practice unlawful on account of being "unfair."[135] In addition to introducing further uncertainty for businesses as to what business practices are covered and how businesses can comply with the requirements of § 5, the absence of any attempt at such an analysis strongly suggests that the FTC will largely focus on the listed "deceptive" business practices. This would be similar to how the FTC has previously approached its regulation of data privacy, where the FTC has generally been hesitant to bring "unfairness" charges absent accompanying charges of "deception."[136] Such an approach is itself likely to encourage businesses to provide increased disclosures to consumers, due to the fact that "deception" charges can be avoided comparatively easily by making such disclosures.

Increased disclosure will be of little benefit to consumers, however, as various information asymmetries make it difficult for consumers to estimate the risks associated with providing their biometric information.[137] Additionally, if the FTC is indeed going to focus primarily on targeting "deceptive" business practices and only bring "unfairness" charges as an addition to "deception" ones, the ability of businesses to avoid "deception" charges by providing disclosures rather than changing their underlying business practices will result in a regulatory regime that is far more reactive than proactive. Absent charges that directly target certain uses of biometric information technologies as "unfair," businesses providing extensive disclosures will likely have a significant amount of free rein to pursue business practices that

---

135 15 U.S.C. § 45(n).

136 Keegan & Schroeder, *supra* note 97, at 28.

137 James P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls or Just More Notice and Choice?*, 37 WM. MITCHELL L. REV. 1727, 1735–38 (2011).

otherwise would be considered "unfair." Such a regulatory regime is especially unsuitable in the realm of biometrics given that the potential harms consumers may face in this area—such as data breaches leading to security vulnerabilities—are nearly impossible to rectify after the fact.[138] Together, these factors suggest that "unfairness" charges, which more directly target harmful business practices themselves rather than the extent to which such practices are disclosed to consumers, are more suited to the regulation of biometric information technologies. The policy statement should thus be revised to contain at least a preliminary cost-benefit analysis balancing the risks associated with a business use of biometrics with the countervailing benefits to consumers or competition, as doing so will fulfill the statutory prerequisites for finding a practice unlawful on account of "unfairness" and thereby embolden the FTC to bring "unfairness" charges even absent accompanying "deception" charges.

A. Scope Issues

As has been shown above, the scope of the policy statement's use of the term "biometric information" (and consequently "biometric information technologies") is far broader than that of even the most expansive state law. The provided definition of "biometric information" in the policy statement covers essentially any conceivable depiction of an individual's physical or behavioral characteristics, and there are also no exclusions provided for information collected in certain contexts, or for certain types of technologies not usually considered to be biometric or not associated with the same uses or risks.

The policy statement's current scope is simply far too broad, and this can be seen by contrasting it with the definitional limitations in the existing state laws to see what technologies excluded in those state definitions may be encompassed by the FTC's regulation here. The most obvious example is photographs, everyday items not commonly considered to be biometric which are specifically excluded from the definition of "biometric identifiers" by both the Illinois BIPA and the WBPA.[139] In contrast, the policy statement specifically lists photographs as an example of

---

[138] *See* Pope, *supra* note 36, at 771–74.

[139] 740 ILL. COMP. STAT. 14/10; 74 WASH. REV. CODE § 19.375.010(1).

biometric information.[140] Another commonplace technology that the policy statement covers is an audio recording of an individual's voice,[141] which is explicitly not considered to be a "biometric identifier" under the WBPA.[142] (It should be noted that these sorts of simple audio recordings are distinct from the more complex "voiceprints" that are considered to be "biometric identifiers" in all three state laws).[143] Finally, even the "written signatures, . . . tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color"[144] excluded from the BIPA's definition of "biometric identifiers" may nevertheless be encompassed by the policy statement's definition, as these types of information "describe . . . traits, characteristics, or measurements of or relating to an identified or identifiable person's body"[145] or, in the case of written signatures, may perhaps describe "characteristic movements or gestures."[146] While considering these types of simple descriptors or identifiers to be "biometric" may seem absurd, the idea was apparently plausible enough to justify being explicitly ruled out in the BIPA. Moreover, the very fact that such an interpretation is conceivable speaks to the unreasonably broad scope of the policy statement in its current form.

Further contributing to the policy statement's overbroad scope is the fact that it does not distinguish between or contain exclusions for information collected in different contexts or for different purposes. There may be technologies which technically record or capture an individual's physical or behavioral characteristics, but do so for reasons entirely unrelated to the purposes of identification and verification usually associated with biometric information technologies. The most obvious example would be medical information gathered in a healthcare context, which is usually intended to be used for some individualized, health-related purpose. As medical information serves a distinct purpose,

---

[140] U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 1 (2023).

[141] *Id.*

[142] 74 WASH. REV. CODE § 19.375.010(1).

[143] 740 ILL. COMP. STAT. 14/10; 11 TEX. BUS. & COM. CODE § 503.001(a); 74 WASH. REV. CODE § 19.375.010(1).

[144] 740 ILL. COMP. STAT. 14/10.

[145] U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 1 (2023).

[146] *Id.*

it has its own sensitivities and risks associated with it, and for that very reason it is already subject to a variety of regulations. The Illinois BIPA and the WBPA recognize this reality by excluding information gathered in such healthcare contexts or for such medical purposes from their definitions of "biometric identifiers,"[147] but the policy statement contains no such limitation for information gathered for this or any other purpose. This omission means that businesses may at worst be subjected to conflicting regulations regarding certain types of information, which again demonstrates how the exceedingly broad scope of the policy statement only serves to increase legal uncertainty for businesses.

The policy statement's current definition does not differentiate between types of information collected for different purposes, and its scope extends far beyond what is usually considered "biometric information" to include commonplace technologies and descriptions not usually thought of as biometric or not associated with the same uses or risks. The current scope is thus clearly far too broad, and this excessively wide scope is almost certain to confuse businesses. To help mitigate this confusion, the FTC should add definitional limitations similar to those found in the existing state laws. Assuming that the FTC wants to adopt the most pro-consumer of these state law approaches, the policy statement should be revised to at least incorporate some of the limitations on scope found in the pro-consumer and relatively strict Illinois BIPA.

B. "Unfairness" Analysis Issues

Initially, the wide variety of practices that the policy statement declares could constitute "deception" or could lead to a finding of "unfairness" under § 5 gives the impression of providing vigorous consumer protections, but this impression is misleading. 1994 amendments to § 5 of the Federal Trade Commission Act declared that the FTC has "no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[148] In the decades following the addition of this "three-part test," the FTC has thus generally

---

147 740 ILL. COMP. STAT. 14/10; 74 WASH. REV. CODE § 19.375.010(1).

148 15 U.S.C. § 45(n).

eschewed from bringing "unfairness" charges and has instead focused primarily on charges of "deception."[149] In regards to the regulation of data privacy, an area which also contains many of the same risks associated with biometrics, "[a]s with other unfairness cases, the substantial majority of the FTC's data privacy cases have also alleged deception—and even more cases have alleged deception without bringing an unfairness charge."[150]

While the policy statement does provide examples of business practices which cause or are likely to cause substantial injury to consumers,[151] as well as a statement of when such harms are not reasonably avoidable,[152] the policy statement does not address when these risks may be outweighed by benefits to consumers or competition and does not perform any sort of explicit cost-benefit analysis. The policy statement does recite the statutory requirement that risks "not [be] outweighed by countervailing benefits to consumers or competition,"[153] but beyond this the closest it comes to addressing this requirement is when it mentions that "the adoption of a contemplated practice may be unjustifiable when weighing the potential risks to consumers against the anticipated benefits of the practice."[154] Specifically, it says that "if more accurate, less risky alternatives are available, using a technology that is proven to have high error rates may present unjustifiable risk to consumers, even if the technology is more convenient, more efficient, or more profitable for the business considering implementing the technology."[155] This is not the precise statutory requirement, however, as § 5 requires weighing the potential risks to consumers against the potential benefits to consumers and competition, not the potential benefits to the business itself.[156] The absence of any sort of cost-benefit analysis is especially striking given the extraordinarily broad scope of the policy statement as outlined above, as presumably the further removed a supposedly covered technology is from those commonly considered biometric, the more exacting the cost-benefit analysis would have to

---

149 Keegan & Schroeder, *supra* note 97, at 19.

150 *Id.* at 28.

151 U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 3–5 (2023).

152 *Id.* at 7.

153 *Id.* at 7.

154 *Id.* at 9.

155 *Id.*

156 15 U.S.C. § 45(n).

be to justify regulating it on "unfairness" grounds. Ultimately, the lack of even an attempt at any cost-benefit analysis seems to suggest that—just as the FTC has done in the recent past with data privacy regulation—the FTC will largely focus on the listed "deceptive" business practices in order to avoid performing the necessary analysis needed to declare business practices unlawful on account of being "unfair."

Additionally, given the FTC's emphasis within the past few decades on increased disclosures in matters of privacy regulation,[157] businesses will most likely be able to avoid the listed "deception" charges by simply providing consumers with additional disclosures. The "unfairness" consideration of "[e]ngaging in surreptitious and unexpected collection or use of biometric information"[158] listed in the policy statement may also be avoidable if businesses simply provide more disclosure. Indeed, the policy statement seemingly encourages disclosure even as a means of limiting exposure to "unfairness" charges, as it states that potential harms to consumers are not reasonably avoidable when, for example, the collection and use of biometric information "is not clearly and conspicuously disclosed."[159] As not being "reasonably avoidable" is one of the three requirements that must be met before the FTC can declare a business practice unlawful on "unfairness" grounds, businesses will likely provide additional disclosures to consumers in order to avoid having their business practices classified as "not reasonably avoidable" and thus more at risk of ultimately being declared "unfair" and unlawful.

The current policy statement will likely incentivize businesses to provide further disclosure—including in advertising—to consumers regarding their biometric information collection practices. This will, however, almost certainly do very little to protect consumers from the risks posed by biometric information technologies. Even when setting aside the usual difficulties with getting consumers to actually read and understand the notice they are provided with, disclosure is particularly ill-suited to address the privacy risks of biometrics for a variety of reasons. This is due to the fact that various information asymmetries make it

---

[157] *See, e.g.*, Maureen K. Ohlhausen, *The FTC's New Privacy Framework*, 25 ANTITRUST 43, 46 (2011).

[158] U.S. FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 10–11 (2023).

[159] *Id.* at 7.

much harder for consumers to estimate the value of private information like biometrics.[160] For example, it is extremely difficult to assess the risks of providing such information when one does not realize how it will ultimately be combined with other information, as information which seems to possess only nominal value from the individual perspective can become extremely valuable in aggregation.[161] Moreover, individuals who do not intuitively grasp the sensitivity of providing certain types of information will also likely not spend significant time evaluating their decision to provide it.[162] Finally, it will frequently be impossible to correlate specific harms with "a particular release of information . . . because information about us resides in so many databases,"[163] further distorting the true cost of providing the information from the individual's perspective and thereby diminishing the effectiveness of increased disclosure.

Furthermore, FTC reliance primarily on "deception" charges and the increased disclosures by businesses that accompany this approach would result in a relatively passive and reactive manner of regulation. Without charges that directly target certain uses of biometric information technologies as "unfair," the ability of businesses to avoid "deception" charges by providing additional disclosures rather than changing their underlying business practices will likely give disclosing businesses a significant amount of free rein to pursue business practices that otherwise would be considered "unfair." This approach is thus not at all suited to the near-irreparable harms that can befall consumers as a result of the mismanagement or misuse of biometric information and biometric information technologies. To take the most obvious example, a data breach that compromises an individual's biometric information immediately compromises all of the individual's data that is locked behind verification technologies using that information, which can frequently include extremely important resources such as financial accounts. Moreover, the unchangeable nature of most biometric information means that the compromised trait is rendered permanently useless for verification purposes going forward. Once such a breach has occurred, any reactive intervention by the FTC will be too late, as the harm to consumers from the theft of their biometric information will have

---

160 Nehf, *supra* note 137, at 1735–38.

161 *Id.* at 1736.

162 *See id.* at 1738.

163 *Id.* at 1737.

already occurred and be almost impossible to rectify. A more proactive regulatory approach is thus required, rather than one which primarily leaves the ball in each individual business's court. Such an approach will likely require substantial "unfairness" charges even absent "deception" ones, as "unfairness" charges more directly target harmful business practices themselves rather than just the extent to which these practices are disclosed to consumers. Given the FTC's past reluctance to bring these sorts of charges in other areas, however, it seems unlikely that it will do so here, which will render the more substantial "unfairness" charges contained in the policy statement much less effective than they otherwise might seem.

The policy statement should thus be revised to include a relatively robust, if ultimately still preliminary, cost-benefit analysis that balances the risks associated with a business use of biometrics with the countervailing benefits. This analysis will need to not only consider the potential harms which may befall consumers as a consequence of a particular business use of biometric information technologies, but also the potential benefits to consumers and competition that may accompany that use. Given the serious nature of the potential harms laid out above, it should not be unreasonably difficult for the cost-benefit analysis to come out in favor of declaring a misuse of biometrics to be "unfair" and thus unlawful, and as a result there is little risk that explicitly performing the analysis will significantly impede necessary regulations. Indeed, by fulfilling the statutory prerequisites, the cost-benefit analysis will in fact embolden the FTC to be much more vigorous in bringing "unfairness" charges even absent accompanying "deception" charges.

C. Likely Business Impact

The extremely broad scope of the policy statement, combined with the lack of any substantial analysis as to when the potential risks associated with a business use of biometric information technologies may be outweighed by benefits to consumers or competition, will create legal uncertainty for businesses by making it unclear which precise business practices are covered and how businesses can comply with the requirements of § 5. The policy statement in its current form, instead of reducing the legal uncertainty in this area, thus merely presents yet another regulation that is inconsistent with others and which businesses must figure out how to comply with.

The various factors laid out in the analysis above will likely result in a bifurcated response to the policy statement between businesses at different economic levels. Smaller businesses for which biometric information is not a major part of their operations will likely scale back on their use of such technologies. This will make it more difficult for these small businesses to compete with larger ones, as it will prevent consumers at the smaller businesses from accessing the conveniences provided by these biometric information technologies, as well as deprive the smaller businesses themselves of the potential cost-savings and efficiencies that come with using these technologies. This competitive disadvantage will only worsen as these technologies improve and become more commercially advantageous for both businesses and consumers. On the other hand, larger businesses for which mass biometric information collection is a major part of their business—such as large tech companies—will likely not scale back their efforts. Instead, they will provide greater amounts of disclosure to consumers regarding their collection practices in an attempt to avoid the policy statement's "deception" charges.

The result of all this is that small businesses—which are already less sweeping in their collection efforts and accordingly less likely to harm consumers—will suffer greater economic costs as a result of the policy statement's inadequacies, while large tech companies with broad biometric information collection efforts which expose consumers to more risk will likely not be impacted. In addition to the obvious competitive harm this would cause smaller businesses, this would almost certainly have a net negative effect on consumers, who would lose out on the economic advantages of having access to biometric information technologies at these smaller businesses without gaining substantial protections from the risk these technologies pose due to the continuing activities of larger companies.

VI. CONCLUSION

The FTC's policy statement inadequately addresses the issues presented by biometric information technologies. Its excessively broad definition of "biometric information" will create significant and unnecessary legal uncertainty for businesses, and the lack of any substantial analysis of when the benefits to consumers or competition of a business use of biometric information technologies are outweighed by the potential risks to consumers (as is required by statute to declare a practice unlawful for being

"unfair") will impede the FTC's ability to bring "unfairness" charges. The policy statement thus indicates—especially when past FTC regulation of data privacy is taken into account—that the FTC will focus primarily on the listed "deceptive" practices, which will likely only lead to an unhelpful and reactive enhanced disclosure regime, as "deception" charges can be somewhat easily avoided by businesses simply by offering more disclosure. To mitigate these twin inadequacies, the FTC should first provide a much more targeted definition of "biometric information" that at minimum incorporates the definitional limitations on scope found in the comprehensive and pro-consumer Illinois BIPA. Such clarification will significantly reduce business uncertainty about the scope of the current policy statement and prevent regulations in this area from unduly burdening technologies that are not commonly considered biometric or associated with the same uses or risks. The FTC should then outline the cost-benefit analysis which will allow it to declare business practices unlawful based on the listed "unfairness" considerations, which will enable a proactive regulatory regime that is better suited to addressing the risks of potentially irreparable harm that consumers face as a result of biometric information technologies.

If these inadequacies are not addressed, the FTC's policy statement will likely disproportionately deter small businesses (thereby harming their prospects in the competitive marketplace) while underregulating the large biometric information collectors that most expose consumers to harm. Consumers will thus be denied economically beneficial access to the commercial benefits of biometric information technologies while simultaneously not being adequately protected from the dangers these technologies pose to their security and privacy. The policy statement therefore requires some retooling if the FTC is to avoid this outcome and strike the right balance between consumer and business interests.