Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act[1]

The increasing use of consumers' biometric information and related marketing of technologies that use or purport to use biometric information ("biometric information technologies")[2] raise significant concerns with respect to consumer privacy, data security, and the potential for bias and discrimination. The Federal Trade Commission is committed to combatting unfair or deceptive acts related to the collection and use of consumers' biometric information and the marketing and use of biometric information technologies.

As used in this document, the term "biometric information" 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. Biometric information 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). Biometric information also includes 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. By way of example, both a photograph of a person's face and a facial recognition template, embedding, faceprint, or other data that encode measurements or characteristics of the face depicted in the photograph constitute biometric information.

Recent years have seen a proliferation of biometric information technologies. For instance, facial, iris, or fingerprint recognition technologies collect and process biometric information to identify individuals. Other biometric information technologies use or purport to use biometric information in order to determine characteristics of individuals, ranging from the individuals' age, gender, or race to the individuals' personality traits, aptitudes, or demeanor. Many biometric information technologies are developed using machine learning or similar data-driven processes that require large quantities of biometric information for "training" or testing purposes.

The Commission has been analyzing consumer protection issues related to biometric information for over a decade. Among other examples,[3] in 2011, as the commercial use of facial

---

[1] This Policy Statement does not confer any rights on any person and does not operate to bind the FTC or the public. In any enforcement action, the Commission must prove the challenged act or practice violates one or more existing statutory or regulatory requirements. In addition, this Policy Statement does not preempt federal, state, or local laws. Compliance with those laws, however, will not necessarily preclude Commission law enforcement action under the FTC Act or other statutes. Pursuant to the Congressional Review Act (5 U.S.C. § 801 et seq.), the Office of Information and Regulatory Affairs designated this Policy Statement as not a "major rule," as defined by 5 U.S.C. § 804(2).

[2] In some contexts, the terms "biometrics" or "biometric technologies" have been used to refer specifically to technologies that are used to identify individuals. We use the term "biometric information technologies" to refer to the broader category of all technologies that use or purport to use biometric information for any purpose.

[3] *See, e.g.*, Press Release, FTC, *FTC to Host Identity Authentication Workshop* (Feb. 21, 2007) https://www.ftc.gov/news-events/news/press-releases/2007/02/ftc-host-identity-authentication-w (announcing a public workshop on topics including biometrics and other emerging authentication technologies); *You Don't Say: An FTC Workshop on Voice Cloning Technologies*, FTC (Jan. 28, 2020), https://www.ftc.gov/news-events/events/2020/01/you-dont-say-ftc-workshop-voice-cloning-technologies.

recognition technology began to take off, the FTC hosted a public workshop, "Face Facts: A Forum on Facial Recognition Technology."[4] The workshop brought together stakeholders from government, academia, and industry to discuss the then-current capabilities and commercial uses of facial recognition technology, as well as potential consumer benefits of and privacy and security concerns about such technology. Following the workshop, in 2012, the FTC published a report entitled "Facing Facts: Best Practices For Common Uses of Facial Recognition Technologies."[5]

Since 2012, some biometric information technologies, such as facial recognition technology, have made significant advances. For example, NIST found that between 2014 and 2018, facial recognition became 20 times better at finding a matching photograph from a database.[6] Such improvements are due in significant part to advancements in machine learning,[7] along with data collection, storage, and processing capabilities sufficient to support the use of these technologies.[8] Simultaneously, many biometric information technologies have become less expensive to deploy.[9] Owing in part to these developments, the use of biometric information technologies is increasingly pervasive. For example, the use of facial recognition and other biometric information technologies in physical locations – such as retail stores, arenas, airports, and other venues – is reportedly growing.[10]

---

[4] FTC, FACE FACTS: A FORUM ON FACIAL RECOGNITION TECHNOLOGY (Dec. 8, 2011), https://www.ftc.gov/news-events/events/2011/12/face-facts-forum-facial-recognition-technology.

[5] FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (Oct. 2012), https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies. Recommendations in this report remain relevant, such as reasonable data security protections for biometric information and appropriate data retention and disposal policies and procedures.

[6] NAT'L INSTITUTE FOR STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 6 (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf; *See also* NIST, Press Release, *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities* (Nov. 30, 2018) https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

[7] *See id.*

[8] *See* A.K. Jain et al., 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters 79 (2016) 100 (stating that "exponential improvements in computing and storage have enabled the deployment of more powerful algorithms to process the captured biometric data" and discussing how, "cloud-based biometrics can facilitate rapid analytics (e.g., recognizing a face using a smartphone camera, where the phone accesses the cloud).")

[9] *See id.* ("[E]xponential improvements in the performance and cost of processors and memory have already played a dominant role in the development of better biometric sensors. . . . In the case of biometric recognition, the direct impact of the rapid improvements in [integrated circuits] is the development of smaller, cheaper, and higher quality biometric sensors.").

[10] *See*, *e.g.*, National Retail Federation and Loss Prevention Research Council, *2022 Retail Security Survey: The State of National Retail Security and Organized Retail Crime*, 17, https://nrf.com/research/national-retail-security-survey-2022 (stating that 12.3% of respondents were implementing or planning to implement facial recognition for loss prevention); *Fast, Frictionless Biometric Payments Gaining Ground in Grocery Stores*, PYMNTS (May 24, 2022) https://www.pymnts.com/news/retail/2022/grocery-stores-will-be-big-winners-this-holiday-season/; Aaron Mok, *These 16 US airports are reportedly testing facial recognition technology on passengers that could roll out nationwide next year*, BUSINESS INSIDER (Dec. 6, 2022) https://www.businessinsider.com/these-16-us-airports-are-reportedly-testing-facial-recognition-tech-2022-12; Kashmir Hill and Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, NYTIMES (Dec. 22, 2022) https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html; Randy Wimbley and David Komer, *Black teen kicked out of skating rink after facial recognition camera misidentified her*,

During this same time period, the use of facial recognition and other biometric information technologies and the risks they pose have been the focus of significant public scrutiny and concern both in the U.S.[11] and abroad.[12] U.S. states and localities have passed laws specifically focused on regulating the commercial use of facial recognition and other biometric information technologies.[13] The requirements in these laws vary – for example, banning the use of facial recognition in certain locations,[14] requiring signs at the entrances of commercial establishments that collect biometric identifiers,[15] or requiring consent to collect biometric information.[16] In 2019 and 2021, the Commission also brought enforcement actions against companies that allegedly misrepresented their use of facial recognition technology.[17]

Consumers, businesses, and society now face new and increasing risks associated with the collection and use of biometric information. For example, biometric information can be used for the production of counterfeit videos or voice recordings (so-called "deepfakes") that would allow bad actors to convincingly impersonate individuals in order to commit fraud or to defame or harass the individuals depicted.[18] Large databases of biometric information may also be attractive targets for malicious actors because of the information's potential to be used for other

---

FOX2DETROIT (July 14, 2021) https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her.

[11] *See*, *e.g.*, *Privacy in the Age of Biometrics: Hearing Before the Subcomm. On Investigations and Oversight of the H. Comm. On Science, Space, and Technology* (2022), https://www.congress.gov/event/117th-congress/house-event/114964?s=1&r=8; *Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy: Hearing Before the House Committee on Oversight and Government Reform* (2020), https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110380; Rebecca Koenig, *New Advocacy Campaign Calls for Banning Facial Recognition on College Campuses*, EDSURGE (Jan. 22, 2020), https://www.edsurge.com/news/2020-01-22-new-advocacy-campaign-calls-for-banning-facial-recognition-on-college-campuses.

[12] *See*, *e.g.*, *Proposal for a Regulation Laying Down Harmonized Rule on Artificial Intelligence*, European Commission, 2021 O.J. (C 206), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence; Global Privacy Assembly, *Adopted Resolution on Facial Recognition Technology*, (2020), https://edps.europa.eu/sites/default/files/publication/final_gpa_resolution_on_facial_recognition_technology_en.pdf

[13] *See*, *e.g.*, Washington Biometric Privacy Protection Act, Wash. Rev. Code § 19.375 (2022) (effective July 23, 2017); Prohibit the Use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland, PORTLAND, OR., CITY CODE Chapter 34.10 (2022) (effective Jan. 1, 2021); Biometric Identifier Information, NEW YORK, N.Y., ADMIN. CODE §§ 22-1201 – 1205 (2023) (effective July 9, 2021). Even prior to 2012, two states, Illinois and Texas, had enacted biometric privacy laws. *See* Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (effective Oct. 3, 2008); Texas Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code § 503.001 (effective Apr. 1, 2009). Additionally, states' comprehensive privacy laws address biometric information. *See, e.g.*, Colorado Privacy Act, 2021 Colo. Legis. Serv. Ch. 483 (S.B. 21-190) (West) (effective July 1, 2023).

[14] PORTLAND, OR., CITY CODE Chapter 34.10 (prohibiting use of face recognition technologies by private entities in places of public accommodation).

[15] NEW YORK, N.Y., ADMIN. CODE § 22-1202(a).

[16] 740 Ill. Comp. Stat. 14/15(b).

[17] Complaint, *In re Everalbum*, FTC File No. 1923172 (May 6, 2021); Complaint, *United States v. Facebook*, No. 19-cv-2184 (D.D.C. July 24, 2019).

[18] For example, in 2020, the Commission hosted a workshop to address the potential benefits and risks to consumers of technology that allows researchers to create a near-perfect voice clone with less than a five second recording of a person's voice. FTC, You Don't Say: An FTC Workshop on Voice Cloning Technologies (Jan. 28, 2020), https://www.ftc.gov/news-events/events/2020/01/you-dont-say-ftc-workshop-voice-cloning-technologies.

illicit purposes, including to achieve further unauthorized access to devices, facilities or data.[19] These issues pose risks not only to individual consumers, but also to businesses and society.[20]

Even outside of fraud, uses of biometric information or biometric information technology can pose significant risks to consumers. For instance, using biometric information technologies to identify consumers in certain locations could reveal sensitive personal information about them—for example, that they have accessed particular types of healthcare, attended religious services, or attended political or union meetings.[21] Moreover, without clear disclosures and meaningful choices for consumers about the use of biometric information technologies, consumers may have little way to avoid these risks or unintended consequences of these technologies.[22]

Some technologies using biometric information, such as facial recognition technology, may perform differently across different demographic groups in ways that facilitate or produce discriminatory outcomes. For example, research 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.[23] The research also found rates of false positives to be higher

---

[19] *See*, *e.g.*, Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Motherboard, VICE (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice; Parmy Olson, *Faces Are the Next Target for Fraudsters*, WALL STREET JOURNAL (July 7, 2021), https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828 (reporting, among other things, the successful hack of a Chinese facial recognition system by fraudsters who uploaded videos they had created from high-definition photographs purchased on the black market). Researchers have reportedly demonstrated techniques for replicating and using non-face biometric identifiers such as fingerprints to circumvent access controls. *See*, *e.g.*, Alex Hern, *Hacker fakes German minister's fingerprints using photos of her hands*, THE GUARDIAN (Dec. 30, 2014), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands. Unauthorized access could also be achieved using synthetic identifiers created by combining biometric information about a large number of individuals. *See* Philip Bontrager et al., *DeepMasterPrint: Generating Fingerprints for Presentation Attacks* (2017), https://www.researchgate.net/publication/317061803_DeepMasterPrint_Generating_Fingerprints_for_Presentation_Attacks.

[20] *See, e.g.*, 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters 79 (2016) 80–105 (discussing that "biometric system[s] may be vulnerable to a number of security threats . . . which may eventually affect the security of the end application."); Bobby Chesney and Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 107 California Law Review 1753, 1758 (2018) (discussing that some harms of deepfakes may be "distortion of policy debates, manipulation of elections, erosion of trust in institutions, exacerbation of social divisions, damage to national security, and disruption of international relations.").

[21] *See* FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES, *supra* n.4, at ii (recommending that businesses consider the sensitivity of information that may be collected by facial recognition systems in light of the locations in which the systems operate).

[22] *See generally* FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES, *supra* n.4, at iii (summarizing recommendations about providing clear notice and choices to consumers about the use of facial recognition technology).

[23] *See* FRVT Demographic Effects in Face Recognition, NAT'L INSTITUTE FOR STANDARDS AND TECH., https://pages.nist.gov/frvt/html/frvt_demographics.html (last accessed Aug. 31, 2022); NAT'L INSTITUTE FOR STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 8: SUMMARIZING DEMOGRAPHIC DIFFERENTIALS (2022), https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf; NAT'L INSTITUTE FOR STANDARDS AND TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 2 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.

in women than men, and in the elderly and children compared to middle-aged adults.[24] 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).[25] 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.[26] 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.[27] 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.

In light of the evolving technologies[28] and risks to consumers, the Commission sets out below a non-exhaustive list of examples of practices it will scrutinize in determining whether companies collecting and using biometric information or marketing or using biometric information technologies are complying with Section 5 of the FTC Act.[29]

---

[24] *Id.*

[25] *See, e.g.,* Joy Buolamwini and Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proceedings of Machine Learning Research 1, 11 (2018) (assessing commercial gender classification systems and finding that all three performed worst for females with darker skin tones).

[26] *See, e.g.*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, EEOC-NVTA-2022-2, THE AMERICANS WITH DISABILITIES ACT AND THE USE OF SOFTWARE, ALGORITHMS, AND ARTIFICIAL INTELLIGENCE TO ASSESS JOB APPLICANTS AND EMPLOYEES (2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence (noting the potential that technologies analyzing the voice will be less accurate for individuals with speech impediments); SELIN E. NUGENT ET AL., INST. FOR ETHICAL A.I., RECRUITMENT AI HAS A DISABILITY PROBLEM: QUESTIONS EMPLOYERS SHOULD BE ASKING TO ENSURE FAIRNESS IN RECRUITMENT 12 (2020) (noting practical considerations that may affect the accuracy of facial analysis technology for individuals with certain disabilities).

[27] *See generally*, Joseph Cox, *How I Broke Into a Bank Account With an AI-Generated Voice*, Motherboard, VICE (Feb. 23, 2023), https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice.

[28] In some instances, biometric information technologies may utilize algorithms and/or artificial intelligence. The guidance below is consistent with and builds on previous publications by the Commission and Commission staff on those topics. *See, e.g.*, FTC, COMBATTING ONLINE HARMS THROUGH INNOVATION (June 2022); FTC, BIG DATA A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (Jan. 2016); Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC: BUS. BLOG (Apr. 19, 2021) https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai; Andrew Smith, *Using Artificial Intelligence and Algorithms,* FTC: BUS. BLOG (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms.

[29] Other laws and regulations enforced by the Commission, including but not limited to the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501–6506) and its implementing Rule (16 C.F.R. Part 312), the Health Breach Notification Rule (16 C.F.R. Part 318), and the Gramm-Leach-Bliley Act's Safeguards Rule (16 C.F.R. Part 314) and Regulation P (12 C.F.R. Part 1016), may also govern the collection, use, or storage of biometric information.

Deception

- ***False or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information***

As with other types of technologies, false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information constitute deceptive practices in violation of Section 5 of the FTC Act.[30] These claims can mislead both individual consumers and businesses that use these technologies. If prospective users rely on false or unsubstantiated claims in choosing one product over another, honest technology vendors who do not oversell their product's capabilities may be placed at a competitive disadvantage. Moreover, if business customers rely on these claims to use technologies that don't work as promised, they may ultimately harm consumers by, for instance, wrongly denying them benefits and opportunities. Thus, the Commission intends to carefully scrutinize claims about these technologies.

As with all marketing claims, the law requires that representations about biometric information technologies be substantiated when made—that is, persons or individuals making such claims must have a reasonable basis for their claims.[31] For example, businesses should be careful not to make false or unsubstantiated claims that technologies are unbiased. Claims of validity or accuracy are deceptive if they are true only for certain populations and if such limitations are not clearly stated.[32] Further, businesses must not make false or unsubstantiated claims about real-world validity, accuracy, or performance of biometric information technologies when the claims are based on tests or audits that do not replicate real-world conditions or how the technology will be operationalized by its intended users.[33] Businesses also should not make false or unsubstantiated claims that the technologies will deliver particular results or outcomes, such as reductions in rates of theft, violent incidents, fraud, or the elimination of bias in hiring.[34]

---

[30] *See* Complaint, *FTC v. Aura Labs, Inc.*, No. 8:16-cv-2147 (C.D. Cal. Dec. 2, 2016) (alleging company's representations that mobile application measured blood pressure with accuracy comparable to a traditional blood pressure cuff were false, misleading, or unsubstantiated); Complaint, *FTC v. New Consumer Solutions, LLC*, No. 1:15-cv-01614 (N.D. Il. Feb. 23, 2015) (alleging company's representations that a mobile application could detect melanoma by analyzing pictures of consumers' skin were false or unsubstantiated).

[31] *See, e.g.*, FTC Policy Statement Regarding Advertising Substantiation, appended to *In re Thompson Med. Co., Inc.,* 104 F.T.C. 648, 839 (1984), *aff'd,* 791 F.2d 189 (D.C. Cir. 1986). Where a company's claims of accuracy, efficacy, or lack of bias refer to specific facts or figures, they must generally be supported by a high level of substantiation, such as scientific or engineering tests. *See also Thompson Med.*, 104 F.T.C. at 822.

[32] *See, e.g.*, Complaint, *In re Everalbum*, FTC File No. 1923172 (May 6, 2021) (alleging company's representations that it was not using facial recognition unless user enabled it were deceptive, where the representations were true only for users in Texas, Illinois, Washington, and the European Union, and users outside of those locations were not provided a setting to turn off facial recognition); *In re J.B. Williams Co., Inc*., 68 F.T.C. 481, 1965 WL 92965, *5 (1965), *aff'd*, 381 F.2d 884 (6th Cir. 1967) (claims that product could reduce fatigue were deceptive, where product was efficacious only in a small minority of cases where tiredness symptoms were due to an iron deficiency, and was of no benefit in all other cases).

[33] *See* Opinion of the Commission at 43-46, *In re ECM Biofilms, Inc.*, FTC File No. 1223118 (Oct. 19, 2015) (laboratory tests performed under aerobic conditions were not competent and reliable evidence of biodegradation in landfills, which are anaerobic environments), *aff'd*, 851 F.3d 599 (6th Cir. 2017).

[34] Claims that "significantly involve. . . safety," as well as claims relating to the performance or other central characteristics of a product or service, are generally material. FTC Policy Statement on Deception (Oct. 14, 1983), appended to *Cliffdale Associates, Inc.,* 103 F.T.C. 110, 174 (1984). *See also* Complaint, *In re Tapplock*, FTC File

- ***Deceptive statements about the collection and use of biometric information***

False or misleading statements about the collection and use of biometric information constitute deceptive acts in violation of Section 5 of the FTC Act, as does failing to disclose any material information needed to make a representation non-misleading. In recent years, the Commission has taken action against businesses that it charged with engaging in deceptive practices related to the collection and use of biometric information.[35] The Commission will continue to carefully scrutinize businesses' conduct in this area to ensure they are not misleading consumers. Businesses should not make false statements about the extent to which they collect or use biometric information or whether or how they implement technologies using biometric information.[36] Businesses also must ensure that they are not telling half-truths—for example, a business should not make an affirmative statement about some purposes for which it will use biometric information but fail to disclose other material uses of the information.[37]

Unfairness

The use of biometric information or biometric information technology may be an unfair practice within the meaning of the FTC Act. Under Section 5, a practice is unfair 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.[38] As discussed above, the collection and use of biometric information can create a serious risk of harm to consumers. Such harms are not reasonably avoidable by consumers if the collection and use of such information is not clearly and conspicuously disclosed or if access to essential goods and services is conditioned on providing the information. For instance, if businesses automatically and surreptitiously collect consumers' biometric information as they enter or move through a store, the consumers have no ability to avoid the collection or use of that information.

Our past cases illustrate that collecting, retaining, or using consumers' personal information in ways that cause or are likely to cause substantial injury, or disseminating

---

No. 1923011 (May 18, 2020) (alleging that representations that smart padlock was secure were deceptive, where padlock had foreseeable information security vulnerabilities and could be quickly unlocked by unscrewing the back panel); Complaint, *FTC v. Lifelock, Inc.*, No. 2:10-cv-00530-MHM (D. Az. Mar. 8, 2010) (alleging that representations that service provided complete protection against all forms of identity theft were deceptive).

[35] *See* Complaint, *In re Everalbum*, FTC File No. 1923172 (May 6, 2021) (alleging that the company misrepresented that it was not using face recognition unless the user enabled it or turned it on); *See also* Complaint, *United States v. Facebook*, No. 19-cv-2184 (D.D.C. July 24, 2019) (alleging that the company misrepresented that users would have to "turn[ ] on" facial-recognition technology, violating a provision of a prior Commission order that prohibited misrepresenting the extent to which users could control the privacy of their data).

[36] *Id.*

[37] *See* Complaint, *United States v. Twitter*, No. 3:22-cv-03070 (N.D. Cal. May 25, 2022) (alleging that statements that users' telephone numbers provided for two-factor authentication would be used for security purposes were deceptive when the company failed to adequately disclose that such numbers would also be used for targeted advertising); Complaint, *In re Sears Holdings Mgmt. Corp.*, FTC File No. 082 3099 (Aug. 31, 2009) (alleging that respondents' statement that they would track consumers' "online browsing" was deceptive in light of failure to adequately disclose tracking of nearly all of the Internet behavior occurring on consumers' computers as well as certain non-Internet related activities taking place on those computers).

[38] 15 U.S.C. § 45(n); *see also* Letter from the FTC to Hon. Wendell Ford & Hon. John Danforth, Ranking Minority Member, S. Comm. on Com., Sci. & Transp., Consumer Subcomm., Comm'n Statement of Pol'y on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in In re Int'l Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984) (the "Unfairness Policy Statement").

technology that enables others to do so without taking reasonable measures to prevent harm to consumers can be an unfair practice in violation of Section 5 of the FTC Act.[39] For example, the FTC has previously charged that businesses have engaged in unfair practices by failing to protect consumers' personal information using reasonable data security practices; by engaging in invasive surveillance, tracking, or collection of sensitive personal information that was concealed from consumers or contrary to their expectations;[40] by, in certain circumstances, implementing privacy-invasive default settings;[41] by disseminating an inaccurate technology that, if relied on by consumers, could endanger them or others;[42] and by offering for sale technologies with the potential to cause or facilitate harmful and illegal conduct like covert tracking, and failing to take reasonable measures to prevent such conduct.[43] Additionally, the FTC has charged that certain discriminatory practices can be unfair.[44] Though many biometric information technologies are new, businesses must continue to abide by longstanding legal requirements and obligations.

In order to avoid liability under the FTC Act, businesses should implement reasonable privacy and data security measures to ensure that any biometric information that they collect or maintain is protected from unauthorized access—whether that access stems from an external

---

[39] *See generally, Privacy and Security*, FTC (last visited Mar. 29, 2023 11:28 AM), https://www.ftc.gov/business-guidance/privacy-security (collecting the FTC's published business guidance related to data privacy and security).

[40] *See, e.g.*, Complaint, *In re Lenovo, Inc.,* FTC File No. 1523134 3134 (Dec. 20, 2017) (alleging that preinstallation of ad-injecting software that, without adequate notice or informed consent, acted as a man-in-the-middle between consumers and all websites with which they communicated was unfair; and that failure to take reasonable measures to assess and address security risks created by the preinstalled software was unfair); Complaint, *FTC v. Vizio, Inc.* Case No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (alleging that collection of sensitive television viewing activity without consent and contrary to consumer expectations, and sharing of such information with third parties, was an unfair practice); Complaint, *In re Showplace, Inc*., FTC File No. 1123151, (Apr. 11, 2013) (alleging that rent-to-own store's use of monitoring and tracking software installed on rented computers was an unfair practice).

[41] *See* Complaint, *United States v. Epic Games, Inc.*, Case No. 5:22-CV-00518 (E.D.N.C. Dec. 19, 2022) (alleging that developing and operating a ubiquitous, freely-available, and internet-enabled video game directed at children and teens that publicly broadcasted players' display names while putting children and teens in direct, real-time contact with others through on-by-default lines of voice and text communication (even after instituting an age gate on the service) was unfair); *see also*, Complaint, *FTC v. Frostwire LLC*, Case No. 111-cv-23643 (S.D. Fla. Oct. 11, 2011) (alleging that distributing an application with default settings that caused or were likely to cause consumers to unwittingly publicly share files already present on, or subsequently saved on, the consumers' mobile devices, including, among others, consumers' pictures, videos, and documents, was an unfair practice).

[42] *See* Complaint, *FTC v. Breathometer, Inc.*, No. 3:17-cv-314 (N.D. Cal. Jan. 23, 2017) (alleging that failing to notify consumers or take corrective action upon learning that device measuring blood alcohol levels was inaccurate was an unfair practice).

[43] *See, e.g.*, Complaint, *In re Support King*, *LLC*, FTC File No. 1923003 (Dec. 20, 2021) (alleging that the provider of software called "Spyfone," which allowed users to surreptitiously monitor and track others' devices, unfairly failed to take reasonable steps to ensure that the purchasers use the monitoring products and services only for legitimate and lawful purposes); Complaint, *In re Retina-X Studios, LLC*, FTC File No. 1723118 (Mar. 26, 2020) (alleging a failure to take reasonable steps to ensure that monitoring products and services that required circumventing certain security protections on mobile devices would be used only for legitimate and lawful purposes by the purchaser); Complaint, *In re DesignerWare, LLC*, FTC File No. 1123151 (Apr. 11, 2013) (alleging that furnishing rent-to-own stores with monitoring and tracking software to be installed on rented computers was an unfair practice).

[44] *See* Complaint, *FTC v. Passport Automotive Group*, Case. No. 8:22-cv-02670-GLS (D. Md. Oct. 18, 2022) (alleging that imposing higher costs on Black and Latino consumers than on similarly situated non-Latino White consumers was unfair); *see also* Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC: BUS. BLOG (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

cybersecurity intrusion or an internal incursion by unauthorized employees, contractors, or service providers.[45] Businesses must also take care that their own collection and use of biometric information is not likely to cause substantial consumer injury.

Determining whether a business's use of biometric information or biometric information technology violates Section 5 requires a holistic assessment of the business's relevant practices. In making such assessments, the Commission will draw on applicable lessons that can be derived from its past work—including, but not limited to, in privacy and data security matters. Importantly, in some situations, the adoption of a contemplated practice may be unjustifiable when weighing the potential risks to consumers against the anticipated benefits of the practice. For example, 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. The Commission's assessment will take into account factors including, but not limited to, the following:

- ***Failing to assess foreseeable harms to consumers before collecting biometric information.***[46] Prior to collecting consumers' biometric information, or deploying a biometric information technology, businesses should conduct a holistic assessment of the potential risks to consumers associated with the collection and/or use.[47] For example, assessments should take into account the context in which the collection or use will take place and the extent to which the specific biometric information technologies to be used have been tested by the business or a third party.[48] The results of testing should be evaluated in light of how well the testing environment mirrors real world implementation and use, including the particular context in which the technology will be deployed. Assessments should also consider the role of human operators. Businesses should not conclude without evidence that the involvement of a human operator is sufficient to mitigate risks to consumers. Businesses should assess whether deploying a biometric information technology system leads to or contributes to outcomes that disproportionately harm particular demographics of consumers. These assessments should take into account

[45] Collecting or retaining biometric information without any legitimate business need or keeping that information indefinitely creates an increased risk of harm to consumers. *See, e.g.*, Complaint, *In re BJ's Wholesale Club, Inc.*, FTC File No. 0423160 (Sept. 20, 2005) (alleging a failure to employ reasonable and appropriate data security measures where, among other things, the company created unnecessary risks to sensitive financial information by storing it for up to 30 days when it no longer had a business need to keep the information); Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging that company created unnecessary risks to personal information by storing it indefinitely on its network without a business need).

[46] *See, e.g.*, Complaint, *In re EPN, Inc.*, FTC File No. 1123143 (Oct. 3, 2012) (alleging a failure to assess risks to consumer personal information it collected and stored online.)

[47] *See, e.g.*, Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 (Dec. 20, 2017) (alleging that respondent's failure to take reasonable measures to assess and address security risks created by third-party software it installed on laptops it offered to consumers was an unfair practice); Complaint, *In re SettlementOne Credit Corp.*, FTC File No. 0823208 (Aug. 17, 2011) (alleging that respondents failed to assess the risks of allowing end users with unverified or inadequate security to access consumer reports through respondents' portal).

[48] *See, e.g.*, Complaint, *In re Upromise, Inc.*, FTC File No. 1023116 (Mar. 27, 2012) (alleging unfair conduct, where defendant allegedly engaged a service provider to develop software that it distributed to consumers but failed, among other things, to assess and address risks posed by the software by testing, post-deployment monitoring, or other means).

whether technical components of the system, such as algorithms, have been specifically tested for differential performance across demographic groups—including intersectionally.

- ***Failing to promptly address known or foreseeable risks,***[49] including by failing to identify and implement readily available tools for reducing or eliminating risks.[50] For instance, if there is evidence that a particular biometric information technology is often prone to certain types of errors or biases, businesses should proactively take appropriate measures to reduce or eliminate the risk that such errors could lead to consumer injury. Steps taken to address risks may include organizational measures, such as policies and procedures to appropriately limit access to biometric information.[51] They may also include technical measures. For example, businesses should timely update relevant systems, including both software components like algorithms and hardware components that are used to capture, process, or store biometric information, in order to ensure that the systems operate effectively and do not put consumers at risk.[52]

- ***Engaging in surreptitious and unexpected collection or use of biometric information.*** [53] In some situations, such conduct may be unfair in and of itself. For instance, businesses may violate the law if they use or facilitate the use of biometric information or biometric information technology to surreptitiously identify or track a consumer in a manner that exposes the consumer to risks such as stalking, exposure to stigma, reputational harm, or

[49] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602, 624-26 (D.N.J. Apr. 7, 2014) (holding that the FTC's complaint adequately stated a claim for unfair data security practices where it alleged, among other things, defendant permitted its hotels to connect insecure servers to its network, including servers with outdated operating systems that could not receive patches to address known security vulnerabilities), *aff'd*, 799 F.3d 236 (3d Cir. 2015); Complaint, *FTC v. Equifax, Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 22, 2019) (alleging failure to implement reasonable procedures to detect, respond to, and timely correct critical and other high-risk security vulnerabilities across Defendant's systems); Complaint, *In re Lookout Services, Inc.*, FTC File No. 1023076 (June 15, 2011) (alleging respondent's failure to adequately assess or address the vulnerability of its web application to widely-known security flaws).

[50] *See*, *e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging a failure to implement readily available protections against well-known and reasonably foreseeable vulnerabilities); Complaint, *In re Compete, Inc.*, FTC File No. 1023155 (Feb. 20, 2013) (alleging a failure to use readily available, low-cost measures to assess/address the risk that data collection software would collect sensitive consumer information it was not authorized to collect).

[51] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging that Residual Pumpkin failed to establish or enforce rules sufficient to make user credentials hard to guess and failed to implement patch management policies and procedures to ensure the timely remediation of critical security vulnerabilities and use of obsolete versions of database and web server software that no longer received patches); Complaint, *FTC v. Equifax, Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 22, 2019) (alleging failure to implement or enforce reasonable access controls to prevent unauthorized access to sensitive personal information).

[52] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC*, FTC File No. 1923209 (June 23, 2022) (alleging failure to implement patch management policies and procedures to ensure the timely remediation of critical security vulnerabilities and use of obsolete versions of database and web server software that no longer received patches).

[53] *See, e.g.*, Complaint, *In re Aaron's, Inc.*, FTC File No. 1223264 (Mar. 10, 2014) (alleging that allowing franchisees to install software facilitating surreptitious collection of private information on rented computers was an unfair practice, and noting that consumers were unable to avoid harm because collection was surreptitious).

extreme emotional distress.[54] Additionally, as discussed above, failing to clearly and conspicuously disclose the collection and use of biometric information makes such collection and use unavoidable by the consumer. Injuries to consumers may also be compounded if there is no mechanism for accepting and addressing consumer complaints and disputes related to businesses' use of biometric information technologies.

- ***Failing to evaluate the practices and capabilities of third parties,*** including affiliates, vendors, and end users, who will be given access to consumers' biometric information or will be charged with operating biometric information technologies. Businesses should seek relevant assurances and contractual agreements that require third parties to take appropriate steps to minimize risks to consumers. They should also go beyond contractual measures to oversee third parties and ensure they are meeting those requirements and not putting consumers at risk.[55] Such oversight may include organizational and technical measures (including taking steps to ensure access to necessary information) to supervise, monitor or audit the third parties' compliance with any requirements.

- ***Failing to provide appropriate training for employees and contractors*** whose job duties involve interacting with biometric information or technologies that use such information.[56]

[54] *See, e.g.*, Complaint, *In re Support King*, FTC File No. 1923003 (Dec. 20, 2021) (alleging that respondents' SpyFone monitoring products and services substantially injure device users by enabling purchasers to stalk them surreptitiously); Complaint, *In re Retina-X Studios, LLC*, FTC File No. 1723118 (Mar. 26, 2020) (similarly alleging respondent's products and services substantially injure device users by enabling purchasers to surreptitiously stalk them); Complaint, *FTC v. EMP Media, Inc.*, No. 2:18-cv-00035 (D. Nev. Jan. 9, 2018) (alleging that defendants published consumers' intimate images without consent in a manner enabling the public to identify or contact the individuals depicted, causing a number of harms to consumers including an unwarranted invasion of privacy into consumers' lives, depression, anxiety, loss of reputation, safety fears, medical and legal costs, and lost time, was unfair)).

[55] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 241 (3d Cir. 2015) (affirming denial of motion to dismiss FTC's complaint alleging unfair data security practices, which included allegations defendant allowed hotel property management systems to connect to its network without taking appropriate precautions, such as ensuring that the hotels implemented adequate information security policies and procedures); Complaint, *In re GeneLink, Inc.*, FTC File No. 1123095 (May 8, 2014) (alleging that company unfairly failed to employ reasonable and appropriate measures to prevent unauthorized access to consumers' personal information because, among other things, it failed to provide reasonable oversight of service providers); *See, e.g.*, Complaint, *In re Upromise, Inc*., FTC File No. 1023116 (Mar. 27, 2012) (alleging failure to take adequate measures to ensure that its service provider employed reasonable and appropriate measures to protect consumer information and to implement the information collection program in a manner consistent with contractual provisions designed to protect consumer information).

[56] *See, e.g.*, Complaint, *In re SkyMed Int'l , Inc*., FTC File No. 1923140 (Jan. 26, 2021) (alleging a failure to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding consumers' personal information); Complaint, *In re Zoom Video Communc'ns, Inc.*, FTC File No. 1923167 (Jan. 19, 2021) (alleging that failure to implement a training program on secure software development principles contributed to unfair conduct).

- ***Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale,[57] or uses[58] in connection with biometric information*** to ensure that the technologies are functioning as anticipated, that users of the technology are operating it as intended, and that use of the technology is not likely to harm consumers.

The Commission notes that a practice need not be equally likely to harm all consumers in order to be considered unfair. In determining what constitutes reasonable practices to protect consumers from potential harms associated with the use of biometric information, therefore, the Commission will—and businesses should—consider the practices from the perspective of any population of consumers that is particularly at risk of those harms.[59]

Finally, the Commission wishes to emphasize that—particularly in view of rapid changes in technological capabilities and uses—businesses should continually assess whether their use of biometric information or biometric information technologies causes or is likely to cause consumer injury in a manner that violates Section 5 of the FTC Act. If so, businesses must cease such practices, whether or not the practices are specifically addressed in this statement.

[57] *See, e.g.*, Complaint, *In re ASUSTeK Computer Inc.*, FTC File No. 1423156 (July 18, 2016) (alleging a failure to perform vulnerability and penetration testing on software that respondent offered for sale, including for well-known and reasonably foreseeable vulnerabilities that could be exploited to gain unauthorized access to consumers' sensitive personal information and local networks).

[58] *See, e.g.*, Complaint, *FTC v. Equifax, Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 22, 2019) (alleging failure to implement reasonable procedures to detect, respond to, and timely correct critical and other high-risk security vulnerabilities across Defendant's systems); Complaint, *In re SettlementOne Credit Corp.*, FTC File No. 0823208 (Aug. 19, 2011) (alleging that respondents failed to implement reasonable steps to maintain an effective system of monitoring access to consumer reports by end users).

[59] *See, e.g.*, Unfairness Policy Statement, *supra* n. 36, at 1074 ("[S]ome may exercise undue influence over highly susceptible classes of purchasers, as by promoting fraudulent 'cures' to seriously ill cancer patients."); Complaint, *In re Philip Morris, Inc.*, 82 F.T.C. 16 (1973) (alleging respondent engaged in an "unfair and deceptive act and practice" by distributing free-sample razor blades in home-delivered newspapers, which posed a particular hazard to young children).