From Fingerprint to Facial Recognition: Compliance Best Practices for Biometric Data Technologies

By Elena Villaseñor Sullivan
November 7, 2024

www.enderezalaw.com | elena@enderezalaw.com | (210) 999-1005

Table of Contents

Introduction

Over the last twenty years, major technology corporations and large financial institutions have leveraged biometric data technology to enhance security, personalize user experiences, and streamline authentication processes. For instance, Apple and major banks have used fingerprint readers and facial recognition to authenticate individuals before accessing their accounts or conducting transactions. Similarly, Amazon's Alexa recognizes different voices to provide personalized reminders, music preferences, and shopping lists. As a result, biometric data technologies are increasingly becoming part of our daily lives and are being integrated into mid-size and smaller businesses. While there are many benefits to using biometric data, companies that use it in their operations should be thoughtful in their development and implementation to minimize their legal and reputational risks.

What are Biometric Data and Biometric Identifiers?

"Biometric data" is generally defined as the raw data collected from an individual's unique physical, biological, or behavioral characteristics, such as images of a face, fingerprints, voiceprints, retina or iris scans, and DNA sequences.[1]

"Biometric identifiers" refer to the specific features or patterns that technology derives from the biometric data that are used to uniquely identify the individual, making it personally identifiable information ("PII").[2] Biometric technologies capture an item of biometric data and then often use technologies with algorithms or database comparison tools to match the data to a particular individual.[3] For example, unique fingerprint patterns, specific measurements of facial features, and distinct voice characteristics.

Federal and state laws vary in how they define biometric data and biometric identifiers, with some definitions conflating the two. The Federal Trade Commission, for example, defines "biometric information" as both the biometric data and the biometric identifiers.[4] The FTC's broad definition of "biometric information" probably aims to regulate the overall intent of using technologies to capture biometric data to automatically authenticate, verify, or create a personal experience for a user.[5] However, litigation has arisen in some contexts to

---

[1] *See* International Bank for Reconstruction and Development/World Bank, *A Primer on Biometrics for ID Systems* (2002), https://id4d.worldbank.org/id-biometrics-primer; *see* U.K. Information Commissioner's Office, *Biometric Recognition*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/ (last visited November 2, 2024); *see* David J. Oberly, Biometrics: *Mitigating Legal Risks When Using Biometric Technologies*, LexisNexis, https://www.lexisnexis.com (last visited November 2, 2024); 740 Ill. Comp. Stat. 14/10.

[2] *See* Innovatrics, *What is Biometrics?*, https://www.innovatrics.com/glossary/biometric-identification/ (last visited November 2, 2024); *see* Thales, *Biometrics* (May 20, 2023), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics; *see* Tex. Bus. & Com. Code Ann. § 11; *see* Wash. Rev. Code § 19.375.010.

[3] *See* Innovatrics, supra note 2; *see* Thales, supra note 2.

[4] Federal Trade Commission (FTC), Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the FTC Act (May 2023), https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-biometric-information-section-5-federal-trade-commission (hereinafter FTC Policy Statement).

[5] *See id.*

determine whether the existing state laws apply biometric data without PII.[6] For example, a Facebook user might upload a picture of an individual who has not registered as a Facebook user, or Alexa might record the voice of an individual who has not enrolled with Amazon, and the companies cannot arguably connect the picture or voice to a unique individual.[7] As discussed below, companies collecting biometric data should follow compliance best practices, even when not processing into PII.

Risks Associated with Biometric Data and Identifiers

As businesses increasingly adopt biometric technologies, it is crucial to recognize and address the associated risks. Understanding these risks is essential for developing effective strategies to mitigate potential legal, ethical, and operational challenges. The following are the top three risks associated with developing and implementing biometric technologies:

1. **Biometric Technology Algorithms**:[8] When developing or licensing biometric technologies, businesses should be cognizant of and mitigate against risks of conscious or unconscious biases in algorithms as well as the human interpretation and use of the data. For instance, facial recognition technologies can have higher error rates for certain demographic groups, leading to misidentification, unfair treatment, and unequal access to services or opportunities, including false arrests, differential marketing practices, and higher insurance premiums.

2. **Privacy and Security:**[9] Biometric data, such as fingerprints, facial recognition, and iris scans, are inherently unique and personalized to each individual, unlike passwords, which can be changed if compromised. This uniqueness makes biometric data, and particularly biometric identifiers, highly sensitive. Collecting biometric information without proper disclosures and user consent could violate the consumer's privacy rights. Additionally, a biometric information breach can lead to irreversible identity theft and fraud. Therefore, companies using biometric technologies should prioritize obtaining informed consent from users and securing the data once captured. Additionally, like other elements of PII, biometric data alone could be breached and combined with other PII to identify an individual, which could lead to identity theft. Therefore, companies collecting biometric data without

[6] *See, e.g.*, Daichendt v. CVS Pharmacy, Inc., No. 22 CV 3318, 2022 WL 17404488, at *5 (N.D. Ill. Dec. 2, 2022) (stating that plaintiffs must "allege that defendant's collection of their biometric data made defendant capable of determining their identities"); Zellmer v. Meta Platforms, Inc., No. 3:18-CV-01880-JD, 2022 WL 976981, at *3 (N.D. Cal. Mar. 31, 2022) (holding that it would be unreasonable to require Facebook to provide notice to, and obtain consent from, non-users who were strangers to Facebook); Wilcosky v. Amazon.com, Inc., 517 F. Supp. 3d 751, 761-62, 757 (N.D. Ill. Feb. 5, 2021) (noting that Alexa recorded the voice of plaintiff, who did not own Amazon Voice ID or purchase an Alexa-enabled device, when she spoke in proximity to another individual's Alexa device); Colombo v. YouTube, LLC, No. 3:22-CV-06987-JD, 2023 WL 4240226, at *3 (N.D. Cal. June 28, 2023) (rejecting the argument that plaintiff must "allege a single fact that would plausibly lead to the conclusion that the data [defendant] collects can be used to identify the individuals in the uploaded videos").

[7] *See, e.g.*, Zellmer, 2022 WL 976981, at *3; Wilcosky, 517 F. Supp. 3d at 761-62, 757.

[8] FTC Policy Statement, supra note 4.

[9] *Id.*

matching it to an individual's identity should still consider the security risks of collecting and storing the data and publicly disclosing such risks.

3. **Surreptitious and Unlawful Uses:**[10] Biometric information is susceptible to use by bad actors for surreptitious and unlawful purposes, such as stalking, harassment, and defamation. Businesses using biometric information are expected to assess such foreseeable risks, disclose them, and mitigate against them.

Addressing the risks associated with biometric data is vital for any organization utilizing these technologies. Businesses can protect themselves and their users by understanding and mitigating the potential biases in algorithms, ensuring robust privacy and security measures, and preventing unlawful uses. Proactively managing these risks helps compile with legal requirements and builds trust and confidence among consumers and stakeholders, ultimately supporting the sustainable and ethical use of biometric data technologies.

Legal Framework

Like most innovations, the laws have not kept up with biometric data technology. Illinois, Texas, and Washington enacted statutes and regulations specific to collecting, using, and storing biometric information, passing legislation in 2008, 2009, and 2017, respectively.[11] Between 2022 and 2024, the legislatures in nine other states introduced bills attempting to regulate biometric data specifically, but none were enacted.[12] However, seventeen states have data privacy laws that include biometric data or biometric identifiers in their definitions of personal information or sensitive data.[13] These data privacy laws broadly require businesses processing biometric data to: (i) conduct data protection assessments, (ii) provide consumers the right to know how their information is being used and a mechanism to correct or delete it, (iii) enter into agreements with specific terms with third parties with whom they who sell, share, or disclose biometric data, (iv) implement security measures, (v) provide notice and gain opt-in consent of consumers prior to collection, and (vi) permit consumers to opt-out of the sale of biometric data and targeted advertising.[14]

---

[10] *Id.*

[11] 740 Ill. Comp. Stat. 14/1 et seq.; 11 Tex. Bus. & Com. Code 503.001 et. seq.; Wash. Rev. Code. Sec. 19.375.010 et. seq.

[12] Ariz. S.B. 1283, 56th Leg., 1st Reg. Sess. (2023); Haw. S.B. 1085, 32nd Leg., Reg. Sess. (2023); Mass. S. 2687, 192nd Gen. Court (2022); Minn. H.F. 2532, 93rd Leg., Reg. Sess. (2023); Miss. H.B. 467, 2023 Reg. Sess.; Mo. H.B. 1584, 102nd Gen. Assemb., 2nd Reg. Sess. (2024); N.Y. A. 1362A, 2023-2024 Reg. Sess.; Tenn. S.B. 339, 113th Gen. Assemb., 1st Reg. Sess. (2023); Vt. H. 21, 2024 Gen. Assemb., Reg. Sess. (vetoed).

[13] Cal. Civ. Code § 1798.140(ae); Colo. Rev. Stat. § 6-1-1303(24); Conn. Gen. Stat. § 42-515(27); 6 Del. C. § 12D-102(30); Fla. Stat. § 501.702(31); Ind. Code Ann. § 24-15-2-28; Iowa Code § 715D.1(26); Md. Code Ann., Com. Law § 14-4701(gg); 2023 Mont. Laws 384, § 2(24); 2024 Neb. Laws 1074, § 2(30); N.H. Rev. Stat. Ann. § 507-H:1(XXVIII); N.J. Stat. § 56:8-166.4; Or. Rev.Stat. Ann. § 646A.570(18); Tenn. Code Ann. § 47-18-3302(26); Tex. Bus. & Com. Code Ann. § 541.001(29); Utah Code Ann. § 13-61-101(32)(a); Va. Code Ann. § 59.1-575 (hereinafter State Data Privacy Law Definitions).

[14] California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act; Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq.; Connecticut Data Privacy Act (CTDPA), Conn. Gen.

Additionally, in May 2023, the Federal Trade Commission announced its Policy Statement on Biometric Data, which asserts that in the absence of a specific biometric data federal statute, the FTC will apply and enforce Section 5 of the FTC Act addressing unfair and deceptive trade practices to the commercial use of biometric data.[15]

Companies should also determine whether the counties or municipalities have enacted ordinances related to biometric data and whether the European Union/European Economic Area's General Data Protection Regulation (GDPR) applies to their operations.

As the regulatory landscape continues to develop, businesses using biometric information in their operations and user experiences should consider combining existing biometric-specific and broader privacy statutes with unregulated best practices to safeguard user privacy and protect against the data's potential misuse and discriminatory impact.

Illinois Biometric Information Privacy Act (BIPA)

In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA), the most comprehensive biometric-specific statute in the United States.[16] BIPA created a private right of action for individuals to pursue class actions for law violations with statutory damages, including the greater of $1,000 or actual damages for negligence and the greater of $5,000 or actual damages for intentional or reckless conduct.[17] Plaintiffs can also recover attorney's fees, costs, and other relief, such as injunctions.[18]

BIPA defines "biometric identifiers" as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, and it defines "biometric information" as any information based on an individual's biometric identifier used to identify an individual.[19] For efficiency in this discussion, "biometric information" will refer to "biometric identifiers" and "biometric information" as defined by BIPA.

BIPA applies to all private entities collecting, using, and storing biometric information.[20] However, it does not apply to biometric information collected for many medical purposes,

---

Stat. §§ 42-515 through 42-526; Delaware Personal Data Privacy Act (DPDPA), 6 Del. C. §§ 12D-101–12D-111, effective Jan. 1, 2025; Florida Digital Bill of Rights (FDBR), Fla. Stat. § 501.701 et seq.; Indiana Consumer Data Protection Act, Ind. Code Ann. §§ 24-15-1-1 through 24-15-11-2; Iowa Consumer Data Protection Act (ICDPA), Iowa Code §§ 715D.1 through 715D.9; Maryland Online Data Privacy Act, Md. Code Ann., Com. Law §§ 14-4701 through 14-4714; Montana Consumer Data Privacy Act, 2023 Mont. Laws 384; Nebraska Data Privacy Act (NDPA), 2024 Neb. Laws 1074; New Hampshire Privacy Act (NHPA), N.H. Rev. Stat. Ann. §§ 507-H:1–507-H:12; New Jersey Data Privacy Act (NJDPA), N.J. Stat. §§ 56:8-166.4 through 56:8-166.19; Oregon Consumer Privacy Act, Or. Rev. Stat. Ann. §§ 646A.570 through 646A.589; Tennessee Information Protection Act, Tenn. Code Ann. §§ 47-18-3301 through 47-18-3315; Texas Data Privacy and Security Act (TDPSA), Tex. Bus. & Com. Code Ann. § 541.001 et seq.; Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq.; Virginia Consumer Data Privacy Act, Va. Code Ann. § 59.1-575 et seq. (hereinafter State Data Privacy Laws).

[15] FTC Policy Statement, supra note 4.

[16] 740 Ill. Comp. Stat. 14/1 et seq.

[17] 740 Ill. Comp. Stat. 14/20.

[18] *Id.*

[19] 740 Ill. Comp. Stat. 14/10.

[20] 740 Ill. Comp. Stat. 14/15.

such as organ donation, material regulated by the Genetic Information Privacy Act and the Health Insurance Portability and Accountability Act, or to validate scientific testing.[21]

In order to collect, use, and store an individual's biometric information, the company must first obtain a written executed release from the individual or their authorized representative after making the following written disclosures:[22]

- The company will collect and/or store the biometric information;
- Identifying the specific purpose for which the biometric information will be collected, stored, and used; and
- The time period for which the biometric information will be used and stored.

BIPA requires companies to implement a written policy made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information.[23] Unless otherwise prohibited by a valid warrant or subpoena, the company must destroy the biometric information on the earlier of the satisfaction of the initial purpose of collecting the information or within three years of the individual's last interaction with the company.[24] The company must store, transmit, and protect biometric information using a reasonable standard of care within the company's industry and in the same manner as or more protective of its other confidential and sensitive information.[25]

Finally, BIPA prohibits companies from selling, leasing, trading, or otherwise profiting from an individual's biometric information.[26]

Texas Capture or Use of Biometric Identifier Act (CUBI)

In 2009, Texas enacted the Capture or Use of Biometric Identifier Act (CUBI).[27] In Texas, there is not a private cause of action for violating CUBI. However, the attorney general may bring an action to recover civil penalties for up to $25,000 per violation.[28] On July 4, 2024, the Texas Attorney General announced that it secured a settlement with Meta for $1.4 billion related to allegations of unauthorized capture and use of facial recognition data without user consent, the first lawsuit brought under CUBI.[29]

---

[21] 740 Ill. Comp. Stat. 14/10.
[22] 740 Ill. Comp. Stat. 14/15(b).
[23] 740 Ill. Comp. Stat. 14/15(a).
[24] *Id.*
[25] *Id.*
[26] 740 Ill. Comp. Stat. 14/15(c).
[27] Tex. Bus. & Com. Code Ann. § 503.001.
[28] Tex. Bus. & Com. Code Ann. § 503.001(d).
[29] Texas Attorney General, Press Release, *Attorney General Ken Paxton Secures $1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data in the Largest Settlement Ever Obtained from an Action Brought by a Single State* (July 30, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture.

CUBI defines a biometric identifier as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.[30] CUBI applies to any person who captures biometric identifiers for commercial purposes, but it does not apply to voiceprint data retained by a financial institution or its affiliate.[31]

To capture a biometric identifier for commercial purposes, the company must get informed consent from the individual before capturing the biometric identifier from the individual.[32] Notably, the statute does not require written disclosure or consent.[33] However, it would be best practice to mitigate the risk effectively.

Once the company captures biometric information, it must comply with three requirements related to (1) selling, leasing, or otherwise disclosing the information, (2) protecting its confidentiality, and (3) destroying the information.

First, the company may not sell, lease, or otherwise disclose the biometric identifier to another person unless:[34]

- The individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;
- The disclosure completes a financial transaction that the individual requested or authorized;
- The disclosure is required or permitted by a federal statute or by a state statute other than the Texas Public Information Act; or
- The disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.

Second, the company must use reasonable care to store, transmit, and protect confidential biometric information from disclosure.[35]

Third, the company must generally destroy the biometric identifier within a year of collecting the information.[36] However, if an employer captures biometric information for security purposes, then the company must destroy the information upon the termination of employment.[37] Additionally, suppose a company uses biometric information in connection with a legally required instrument or document. In that case, the company must destroy the information upon the expiration of a year after that document is required to be retained by law.[38]

---

[30] Tex. Bus. & Com. Code Ann. § 503.001(a).
[31] Tex. Bus. & Com. Code Ann. §§ 503.001(b) and (e).
[32] Tex. Bus. & Com. Code Ann. § 503.001(b).
[33] *See Id.*
[34] Tex. Bus. & Com. Code Ann. § 503.001(c)(1).
[35] Tex. Bus. & Com. Code Ann. § 503.001(c)(2).
[36] Tex. Bus. & Com. Code Ann. § 503.001(c)(3).
[37] Tex. Bus. & Com. Code Ann. § 503.001(c-2)
[38] Tex. Bus. & Com. Code Ann. § 503.001(c-3).

Washington Biometric Privacy Law

In 2017, Washington enacted legislation specific to biometric information.[39] The law is enforced by the Washington Attorney General and can result in monetary fines of up to $500,000 and compensation for the harm caused.[40]

In Washington, a "biometric identifier" means 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 used to identify a specific individual.[41] It does not include a physical or digital photograph, video or audio recording, or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.[42]

Notably, the statute only applies to biometric identifiers collected and used in furtherance of a sale or disclosure to a third party to market goods or services.[43] It does not apply to collection and use to prevent shoplifting, fraud, security, or law enforcement.[44]

A person may only enroll a biometric identifier in a database for commercial purposes after first providing notice readily available to the individual, obtaining affirmative consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.[45] While the type and content of the notice depend on the context, a company that obtains a biometric identifier may not use or disclose it in a manner that is materially inconsistent with the terms of the notice.[46]

Companies that obtain biometric data must destroy the identifier when it is no longer necessary to provide the services for which the biometric identifier was obtained, except to comply with a court order, statute, or public records retention schedule specified by law or to protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability.[47]

Additionally, a company may not sell, lease, or otherwise disclose a biometric identifier to a third party unless the company has met the notice and consent requirements related to the sale, lease, or disclosure; the disclosure is necessary to provide a product or service specifically authorized by the individual or to effect a financial transaction that the individual requests; the disclosure is required by law or to participate in litigation; or the third party to

[39] Wash. Rev. Code § 19.375.010 et seq.
[40] Wash. Rev. Code § 19.375.020.
[41] Wash. Rev. Code § 19.375.010.
[42] *Id.*
[43] Wash. Rev. Code §§ 19.375.010(4), 19.375.020(6).
[44] Wash. Rev. Code §§ 19.375.010(4) and (8), 19.375.020(7).
[45] Wash. Rev. Code §§ 19.375.020(1) and (2).
[46] Wash. Rev. Code §§ 19.375.020(2) and (5).
[47] Wash. Rev. Code § 19.375.020(4)(b).

whom the biometric identifier is disclosed contractually promises confidentiality unless it meets the notice and consent requirements described above.[48]

State Privacy Statutes

Seventeen states have enacted data privacy legislation that includes biometric data in their definition of the "personal information" or "sensitive data" that companies must protect.[49] While each state data privacy law has its own unique features, generally, those laws require the following as it pertains to all "personal information" or "sensitive data," including biometric data:[50]

1. **Data Protection Risk Assessments.** Companies must conduct and document a data protection risk assessment, particularly when they sell sensitive data or intend to use the biometric data for targeted advertising, profiling, and similar heightened risks. Generally, risk assessments must weigh the risks, benefits, and contexts of collecting and processing the biometric data, how data might be de-identified, and the reasonable expectations of consumers.
2. **Security Measures.** Companies must minimize the biometric data collected to be proportionate to the purpose of collection, refrain from secondary uses of the biometric data without proper disclosure of those uses, and implement security measures to protect the data.
3. **Transparency and Notice.** At or before collecting biometric data, the company must inform consumers that biometric data will be collected, the purpose of collecting the biometric data, whether the biometric data will be sold or shared, and the company's retention time period for the biometric data.
4. **Opt-Out.** Companies must provide consumers with the ability to opt-out of targeted advertising, sale of biometric data, and profiling.
5. **Consumer Rights to Records, Modification, and Deletion.** Companies must notify consumers of their privacy rights and provide a secure mechanism for consumers to easily request biometric data records or to modify or delete their biometric data records, including authentication of the requesting consumer's identity. Additionally, companies must respond in a manner and time period that is reasonable (typically less than 45 days by mail, email, a toll-free number, webpage customer web portal).
6. **Third Party Contracts.** Companies must enter into written contracts with third-party data processors and suppliers that will have access to biometric data to detail the third party's responsibilities and ensure that the third party will care for the biometric data in the same way that the company is responsible for complying. The contract should include provisions requiring the third party to refrain from disclosing, selling, or

[48] Wash. Rev. Code § 19.375.020(3).
[49] State Data Privacy Law Definitions, supra note 13.
[50] State Data Privacy Laws, supra note 14.

transferring the biometric data without the consumer's consent and provide biometric data security to ensure its protection and confidentiality.

States vary in the types of enforcement and liability exposure for breaches of their data privacy laws. Some states enforce through Attorney General actions, others through private rights of action, and sometimes both remedies are available.[51]

Federal Law

No comprehensive or targeted federal law governs the capture, use, and destruction of biometric data. As a result, the Federal Trade Commission (FTC) has asserted its role as the federal regulator on consumer protection in the area of privacy and security of biometric data through Section 5 of the FTC Act, which prohibits "unfair methods of competition" and "unfair or deceptive trade practices."[52] In May 2023, the FTC adopted a Biometric Policy Statement.[53] The Policy Statement is not a binding regulation. Instead, it states the FTC's position on how Section 5 of the FTC Act applies to biometric technologies.

Following the issuance of its Biometric Policy Statement, the FTC announced in May 2023 that it was pursuing three enforcement actions targeting the improper use of biometrics. In addition to requiring the defendants to implement widescale corrective action measures, the enforcement actions resulted in the following settlement penalty payments:

- Amazon agreed to pay a $25 million civil penalty related to its Alexa voice assistant service;[54]
- Ring agreed to pay a $5.8 million civil penalty related to the company's collection, storage, and analysis of video data captured by Ring devices; [55]
- Meta agreed to pay a $5 billion civil penalty related to how Meta could use children's and teens' information;[56] and
- Rite Aid agreed to refrain from using facial recognition for security and surveillance purposes for five years.[57]

---

[51] *See id.*
[52] FTC Policy Statement, supra note 4; 15 U.S.C. § 45.
[53] *Id.*
[54] U.S. Dep't of Justice, Press Release, *Amazon Agrees to Injunctive Relief and $25 Million Civil Penalty for Alleged Violations of Children's Privacy* (May 31, 2023), https://www.justice.gov/opa/pr/amazon-agrees-injunctive-relief-and-25-million-civil-penalty-alleged-violations-childrens.
[55] Fed. Trade Comm'n, Press Release, *FTC Says Ring Employees Illegally Surveilled Customers and Failed to Stop Hackers from Taking Control of Users' Accounts* (May 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users.
[56] Fed. Trade Comm'n, Press Release, *FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (May 2023)*, https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data.
[57] Fed. Trade Comm'n, Press Release, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Consent* (Dec. 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

While not exhaustive, the FTC's May 2023 Biometric Policy Statement addresses the primary areas where a company's collection, use, and storage and representations about its collection, use, and storage of biometric data may violate Section 5.[58] The FTC will focus its enforcement efforts on the following acts that it has deemed an unfair and deceptive trade practice under Section 5:[59]

1. **False or unsubstantiated marketing claims** relating to biometric technologies' validity, reliability, accuracy, performance, fairness, or efficacy. Examples:
    - Claims that the technology is unbiased, if it is valid for only certain populations and if such limitations are not clearly stated.
    - Claims about the technology's validity, accuracy, and performance when the tests or audits are not based on real-world conditions.
    - Claims that the technology delivers particular results or outcomes, such as reductions in theft, violence, fraud, or eliminating bias in hiring when the tests or audits have not substantiated such claims.
2. **Deceptive representations and omissions** regarding the collection and use of biometric information. Examples:
    - Misrepresenting that the company only uses face recognition if the individual enables it or turns it on.
    - Failing to disclose that the collection and use of biometric information has the risk of consumers using it for covert or unlawful purposes such as stalking or harassment.
    - Misrepresenting that the use reduces consumer costs when the data derived from the technology might be used to increase costs for certain classes of consumers.
3. **Failing to assess foreseeable harm and address known or foreseeable risks** to consumers before collecting biometric data. Examples:
    - Failing to conduct an in-house or third-party real-world assessment of the technology's performance, such as:
        - Using an inaccurate context in which collection or use will take place;
        - Failing to take the extent of use into account;
        - Failing to evaluate whether outcomes lead to disproportionate harm for particular demographics of consumers; and
        - Failing to assess whether the controls sufficiently mitigate the consumer risk, avoiding human operator involvement as the sole control.

[58] FTC Policy Statement, supra note 4.
[59] *Id.*

- Failing to proactively identify and implement readily available tools for reducing or eliminating risks.
- Failing to adopt policies and procedures to limit access to biometric data appropriately.
- Failing to update systems in a timely manner to ensure they operate effectively and protect against data breaches.

4. **Engaging in the surreptitious and unexpected collection or use of biometric information**. Examples:
    - Using biometric data in a manner that exposes consumers to risks such as stalking, exposure to stigma, reputational harm, or extreme emotional distress.
    - Failing to take security measures to reduce the risk.
    - Failing to have a mechanism to address consumer complaints relating to such risk.
5. **Failing to evaluate the practices and capabilities of third parties**. Examples:
    - Failing to have a third-party risk management program in place to ensure that third parties, including affiliates, will be given access to consumers' biometric data or will maintain responsibility for operating biometric technologies that meet contractual and legal requirements.
    - Failing to provide appropriate training for employees and contractors.
    - Failing to conduct ongoing monitoring of biometric technologies for continued intended functionality and proper usage.
6. **Failing to provide appropriate training** for employees and contractors whose job duties involve interacting with biometric information or technologies that use such information.
7. **Failing to conduct ongoing monitoring of technologies that the business develops**, offers for sale, or uses 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.

Consolidated Action Plan for Biometric Data Compliance

Given biometric data regulations' diverse and evolving landscape, businesses must adopt a comprehensive and proactive approach to compliance. While the laws impacting biometric data vary, there are common overlapping themes. This action plan consolidates the most stringent laws and highest requirements from various jurisdictions to provide a robust framework for managing biometric data. As a result, companies should conduct regular data security risk assessments and audits in compliance with applicable federal and state privacy statutes and regulations, even if they are outside of the area in which these companies operate. Adhering to high standards will help ensure compliance across multiple regions, mitigate legal and reputational risks, and build trust with consumers and stakeholders. The following steps outline key areas such as technology evaluation, risk mitigation, data security, and regulatory adherence, offering a thorough approach to responsible biometric data management.

1. **Evaluate Underlying Technology Infrastructure and Performance**
   Conduct an independent real-world assessment of the technology's models, algorithms, and performance, including:
   - Understanding the assumptions built into the technology.
   - Assessing whether the technology's application and outcomes are appropriate for the accurate context for data collection and use.
   - Evaluating the technology's output for implicit bias and disproportionate outcomes.

2. **Conduct Data Protection Risk Assessments**
   Regularly conduct and document data security risk assessments and audits in compliance with state data privacy statutes. The assessments should weigh the risks and benefits in the real-world context of collecting and processing biometric data, including those relating to the sale or transfer of biometric data and the use of biometric data for targeted advertising, profiling, and similar heightened risks.

3. **Mitigate Internal Risks**
   Before launching biometric technology, implement measures to address known or foreseeable risks, including policies and procedures, and proactively identify and use tools to reduce or eliminate risks. Use process, legal requirements, and control mapping to ensure that all operational "touchpoints" are evaluated.
   - Collection and use should be limited to the methods and means described in the company's notice and consent (as described further below).
   - Evaluate whether human involvement in interpreting or acting upon biometric information could lead to disproportionate harm for particular demographics.
   - Identify and mitigate against the technology's foreseeable surreptitious and unlawful uses, including stalking, harassment, and defamation.
   - Implement policies, procedures, and controls for de-identifying biometric data.

- Develop and implement procedures and controls to identify and escalate new processes, technologies, channels, and functions related to biometric information so that the proper policies, procedures, and controls can be updated and applied accordingly.

4. **Limit the Sale, Lease, and Trade of Biometric Information to Third Parties**
   Prohibit the sale, lease, trade, and profit (collectively, "transfer") from biometric data for Illinois consumers. In other jurisdictions, only transfer biometric data in the following circumstances:
   - With the individual's consent;
   - To complete a financial transaction requested by the individual;
   - To comply with other laws or valid subpoenas and court orders;
   - For law enforcement purposes;
   - To prevent fraud or criminal activity (Washington).

5. **Implement a Retention and Destruction Policy**
   Develop and implement an internal policy that mandates the destruction of biometric information and procedures and controls to operationalize the policy. The company must destroy biometric information upon the earlier of:
   - The satisfaction of the initial purpose of the collection; or
   - As prescribed by specific state laws. Examples:

     <u>Texas</u>
     - Within 1 year of collection;
     - If collected by the employer for security purposes upon termination of employment; or
     - If collected for a legally required instrument within 1 year of the legally required retention period for that instrument.

     <u>Illinois</u>
     - Within 3 years of the last interaction with the company; or
     - As permitted by a warrant or subpoena.

     <u>Washington</u>
     - As permitted by court order, statute, or public record retention schedule; or
     - As long as needed to protect against fraud, criminal activity, claims, security threats, or liability.

6. **Ensure Marketing and Representations are Fair and Accurate**
   Ensure the marketing department can substantiate claims related to the technology's validity, reliability, accuracy, performance, fairness, and efficacy. Review representations about the collection and use of the biometric data to ensure they are accurate and complete.

7. **Secure Biometric Data**
   Use the reasonable standard of care within your industry to store, transmit, and protect biometric data, ensuring the company protects biometric information like other company confidential and sensitive information, including:

   - **Encryption**: Ensure that biometric information is encrypted in transit and at rest to protect against unauthorized access.
   - **Access Controls**: Implement strong security measures to prevent unauthorized access and data breaches. Limit access to only those employees and third parties who need it to perform their job functions.
   - **Regular Monitoring**: Continuously update systems to ensure they operate effectively and protect against potential security threats and vulnerabilities.

8. **Publish a Publicly Available Data Privacy Policy**
   Prepare and make publicly available in a location easily accessible to affected individuals a Privacy Policy that addresses the following:
   - The company's notice and consent policy;
   - A retention schedule for biometric information;
   - Methods for consumers to easily request their biometric data or to modify or delete their biometric data using mail, email, a toll-free number, a webpage, or a customer portal;
   - The company's process to review and respond to the requests for records, deletion, or modification within a forty-five-day period; and
   - Guidelines for permanently destroying biometric information.

9. **Provide Notice, Opt-Ins, and Opt-Outs Before Biometric Data Collection**
   - **Obtain Written Affirmative (Opt-In) Consent**: Secure written affirmative (opt-in) consent from the consumer in a location readily available and in a manner that is understandable to the average consumer. The written notice prior to obtaining consent should include the following information to put the affected individual on notice of the company's collection, use, and storage of their biometric data:
     - The company will collect, use, and store their biometric data.
     - The specific purpose for which the company will collect, use, and store their biometric data, including using biometric identifiers.
     - Whether the company will sell, lease, trade, or profit from the biometric data;
     - Where permitted by law, whether the company will disclose biometric information to third parties, how third parties will use the data, and the controls in place to ensure the third party maintains confidentiality of the biometric information.
     - The time period for which the company will store and use the biometric data.

- **Opt-Out.** Provide consumers with the ability to opt-out of targeted advertising, sale of biometric data, and profiling.

10. **Implement a Consumer Request and Complaint Process**
    Implement a mechanism for consumers to easily request their biometric data, request modification or deletion of their biometric data, and submit complaints about the collection, use, storage, or breach of their biometric data. Ensure there is an operational process and adequate staff to review requests and complaints and promptly act on them in less than forty-five days, including assessing whether requests and complaints signal weaknesses in controls.

11. **Train Employees and Third Parties**
    Train employees and third parties on:
    - The benefits and risks of collecting and using biometric data;
    - The laws related to biometric data technologies and the consequences of non-compliance;
    - Policies and procedures;
    - Controls to mitigate the risks; and
    - Reporting violations or potential risks.

12. **Monitor, Test, Audit**
    Develop a system to monitor ("micro-test") the effectiveness of controls on a regular frequency, depending on the level of risk. Conduct independent larger-scale tests/audits at intervals proportionate to the overall risks.

13. **Effectively Manage Noncompliance through Issue Management**
    Have a process in place to collect and memorialize compliance gaps that are self-reported or identified through complaints, monitoring, or testing/audits, including a process to prioritize compliance gaps. Ensure adequate staff and that it is a company priority to close compliance gaps.

14. **Manage Third-Party Risk**

    - **Due Diligence**: Conduct thorough due diligence before engaging with third parties who will have access to or process biometric data, including evaluating their data protection practices, compliance history, and reputation. Verify their policies, procedures, and controls used to comply with biometric data laws.
    - **Contractual Agreements**:
        - Include specific clauses in third-party agreements requiring compliance with biometric data laws, including data collection, use, storage practices, the sale or transfer of biometric data, security measures, and data retention and storage policies.

- Require third parties to have and share their incident response plan for data breaches and to promptly notify the company of any data breaches or compliance issues.
- Ensure that the company has the right to monitor, test, and audit the third party's compliance with biometric data laws.

- **Training**: Ensure the third party knows and understands the legal requirements and risks associated with biometric data, as well as your company's policies to address those risks.
- **Monitoring and Testing/Audits**: To ensure ongoing compliance, conduct regularly scheduled monitoring activities and scheduled and surprise audits.

15. **Prepare for Data Breaches**
    Ensure the company's data breach response plan includes specific steps for addressing breaches involving biometric data.

By implementing this consolidated action plan, businesses can confidently navigate the complexities of biometric data compliance. This plan addresses the highest regulatory standards and incorporates best practices that enhance data security and privacy. These measures will help companies mitigate risks, ensure legal compliance, and build stakeholder trust. A proactive and comprehensive approach to biometric data management will ultimately support sustainable and ethical business practices in an increasingly data-driven world.

Conclusion

As biometric data technologies continue to evolve and become integral to various business operations, it is imperative for companies to navigate the complex regulatory landscape with diligence and foresight. The legal frameworks established by states like Illinois, Texas, and Washington and federal oversight by the FTC underscore the importance of protecting biometric information. Businesses can mitigate legal and reputational risks by implementing comprehensive compliance strategies, including robust data security measures, transparent notice and consent practices, and thorough third-party risk management. Adhering to best practices ensures compliance with current laws and fosters trust and confidence among consumers. As the use of biometric data expands, staying informed and proactive in addressing potential risks will be crucial for maintaining ethical and lawful operations.