

The Growing Risks of Collecting and Using Biometric Data: Regulations in New York and Elsewhere

June 21, 2023

"Biometric Data" is currently one of the hottest buzzwords in the cybersecurity and privacy realms. The term refers to various personal characteristics that are used to identify an individual, such as physical and biological traits like fingerprints, retina patterns, and other facial features, as well as behavioral characteristics like handwriting or an individual's gait. Biometric data points are used to verify and authenticate an individual's identity to gain access to software or hardware and access control security measures. Biometric data has increasingly become a preferred method for preventing fraud, theft, and other activities frequently perpetrated by malicious actors—over traditional security mechanisms like user IDs, passwords, and PINs.

As a result of the increased use of biometric data for privacy and security, both states and cities (such as NYC) have proposed and enacted regulations that mandate certain safeguards to protect the biometric data of individuals that is collected and maintained by businesses, and some laws allow for private rights of action. This has manifested in significant regulatory enforcement actions as well as private causes of action (including class actions). It is vital that entities that collect and maintain biometric data understand the applicable regulations and associated litigation and regulatory risks and have policies and safeguards in place to ensure compliance.

New York Regulations Protecting Biometric Data

The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act is a data security law that regulates the protection of personal information, including biometric data, and includes data breach notification obligations. The SHIELD Act expanded the scope of "private information" to include biometric data, defined as "data generated by electronic measurements of an individual's unique physical characteristics" (which includes fingerprints, voiceprints, and retina or iris images). The SHIELD Act applies to all entities (including businesses and nonprofits) that collect private information of New York residents, regardless of whether the company transacts business in New York, and requires that they implement reasonable data security measures with administrative, technical, and physical safeguards to protect that information from unauthorized access, use, modification, or disclosure. Additionally, the SHIELD Act mandates that businesses notify affected individuals and the New York Attorney General in the event of a data breach that involves personal data, including biometric information.

Another New York regulation, the Department of Financial Services (DFS) Cybersecurity Regulation, provides a comprehensive framework for covered entities to protect sensitive information, like biometric data, from cyber threats. It requires covered entities to establish policies and procedures for risk assessment, data protection, incident response, and employee training to safeguard the confidentiality, integrity, and availability of biometric data in the financial services industry. Accordingly, financial institutions and other covered entities operating in New York State, including banks and trust companies, insurance companies, mortgage brokers, investment companies and advisers, and credit unions, must comply with the NY DFS Cybersecurity Regulation and take appropriate measures to protect biometric data as part of their overall cybersecurity framework. They are also required to report any cybersecurity incidents affecting their operations or involving sensitive information like biometric data to the NY DFS within 72 hours of discovery.

New York City enacted a biometric data privacy law in 2021, the New York City Biometric Identifier Information Law.^[1] This law applies to any commercial establishment that collects, retains, converts, stores, or shares biometric identifier information of customers, and requires that businesses disclose to customers such collection, retention, conversion, storage, or sharing of their biometric data by placing a clear and conspicuous sign in plain and simple language near all customer entrances to serve as notice. It prohibits the selling, leasing, or profiting from consumers' biometric data. The law provides for a private right of action and allows for damages of \$500 for each violation and negligent violation of the regulation, \$5,000 for each intentional or reckless violation of the regulation, attorneys' fees and other related costs and expenses, and other forms of relief including an injunction. However, commercial establishments must be given written notice with a 30-day cure period to correct any violation and allows alleged violators the opportunity to avoid liability if they cure, provide the aggrieved individual an express written statement that the violation was cured, and have no further violations.

In addition, New York State lawmakers proposed a statewide biometric privacy act.^[2] This law, which is still in committee and must pass both the Senate and Assembly, would require private entities that maintain biometric information of individuals to develop a written policy with a retention schedule and guidelines for properly destroying individuals' biometric information once no longer needed for its original collection purpose or within three years of the individual's last interaction with the entity. Currently, it is unclear of the jurisdictional limits of this law and whether it would only apply to New York private entities or only apply to the biometric information of New Yorkers. Further, the law would allow for a private right of action with damages ranging from \$1,000 to \$5,000 per violation, or more for actual damages.

Other States' Proposed Legislation Regulating Biometric Data

As of this year, 11 U.S. states (like New York) have proposed specific biometric data privacy laws that would impose requirements on businesses' collection, use, and protection of individuals' biometric information. These proposed bills increase the compliance risk and liability exposure of businesses that collect individuals' biometric information. For example, Illinois, Texas, and Washington have enacted specific biometric data privacy laws to regulate the use and disclosure of biometric data to protect individuals' sensitive information.^[3] Tech giant Google has already been subject to a lawsuit by the Texas Attorney General for violating the Texas Capture or Use of Biometric Information Act by allegedly collecting from Google apps and devices and indefinitely storing large amounts of Texans' facial and voice recognition data, including facial geometry and voiceprints, without knowledge or consent.^[4]

Illinois's Biometric Information Privacy Act is currently the only enacted narrow biometric data law that currently provides a private right of action against noncompliant businesses, in addition to penalties and injunctive relief. There have been numerous suits in Illinois brought under this law against tech titans such as Google, TikTok, and Snapchat, resulting in settlements of up \$100 million, \$92 million, and \$35 million, respectively.^[5] And, in October 2022, a jury trial resulted in a \$228 million verdict against BNSF Railway Co. in connection with its practice of fingerprinting drivers without notice and consent, and was calculated based on a finding of 45,600 violations (multiplied by \$5,000 per class member).^[6]

Washington recently passed the My Health My Data Act on April 27, 2023, which is the broadest such law to date, providing a private cause of action and having extraterritorial application, and becomes effective in 2024.^[7] Under Washington's My Health My Data Act, a "regulated entity" is broadly defined as any legal entity that conducts business within the state or "produces or provides products or services that are targeted to consumers in Washington" (including entities outside of the state). Thus, for example, New York businesses that advertise to Washington consumers may be sued in Washington for violations of this law. Additionally, the law defines "biometric data" significantly broader than other federal and state privacy laws such that the law may apply to some businesses that do not consider themselves to collect health information.

Some other state laws are narrowly tailored, such as a 2022 Colorado law that restricts the use of facial recognition technology by government agencies.^[8]

Comprehensive Privacy Laws

Biometric data regulation is further covered by comprehensive state data privacy laws, often as a highly protected form of sensitive personal information. New York has proposed legislation aimed at regulating entities that collect or process the personal data of New Yorkers as well as providing protective consumer rights, and, as proposed, includes biometric data.^[9] As of June 2023, nine states (California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Montana, and Tennessee) have successfully enacted comprehensive state privacy laws that protect consumers by providing them certain rights to control their personal data and regulate businesses' use of consumers' personal data, including a special category of sensitive information which covers biometric data.^[10]

While the comprehensive state privacy laws are jurisdictional and depend on the collection and processing of personal data in that particular state, the General Data Protection Regulation (GDPR) regulates businesses located anywhere in the world that handle the personal data of EU residents and also provides consumer rights to those EU residents. The EU GDPR took effect on May 26, 2018, is the strictest of all comprehensive privacy laws, and covers biometric data.^[11] The UK GDPR, which took effect on January 1, 2021, contains mostly identical provisions applicable to UK residents' personal data.^[12]

Distinction in Scope and Future Applicability

Whether an entity is covered by narrowly tailored biometric data privacy laws or comprehensive data privacy laws that apply to biometric data, it is imperative that entities that collect or maintain such data understand their obligations and have policies in place to ensure compliance. Several state and federal agencies with the requisite enforcement power have begun to crack down on companies of all sizes for privacy violations.

With over 20 U.S. states having recently proposed comprehensive privacy legislation, several states with currently effective data privacy laws, and some states and cities with specific laws relating to biometric data, it is crucial for all businesses to reconsider their current practices and policies concerning biometric data, assess the laws that may be applicable now or in the future, and ensure compliance.

* * *

^[1] New York City Biometric Identifier Information Law, N.Y.C. Admin. Code § 22-1201 *et seq.*

^[2] A1362, 2023-2024 Legis. Sess. (N.Y. 2023) (Add Art 32-A §§676 – 676-d, Gen Bus L); S4457, 2023-2024 Legis. Sess. (N.Y. 2023) (Add Art 32-A §§676 – 676-d, Gen Bus L).

^[3] Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (eff. Oct. 3, 2008); Tex. Bus. & Com. Code Ann. § 503 (eff. Apr. 1, 2009); Wash. Rev. Code § 19.375.010, *et seq.* (eff. July 23, 2017).

^[4] *United States v. Amazon.com, Inc.*, Case: 2:23-cv-00811 (W.D. Wash. May 31, 2023).

^[5] *See Rivera v. Google LLC*, Case No. 2019-CH-00990 (Ill. Ct. Cl. Apr. 14, 2022); *In Re TikTok, Inc., Consumer Privacy Litigation*, Case: 1:20-cv-04699 (N.D. Ill. July 28, 2022); *Boone v. Snap Inc.*, Case No. 2022LA000708 (8th Cir. Aug. 4, 2022).

^[6] *See Rogers v. BNSF Railway Co.*, Case No. 1:19-cv-03083 (N.D. Ill. Oct. 12, 2022).

^[7] Washington My Health My Data Act, 2023 Wash. Sess. Laws Ch. 191 (eff. July 23, 2023).

[8] Colo. Rev. Stat. add § 2-3-1707; add (18.5)(a)(III) § 2-3-1203; amd § 2-3-1701; add Part 3 Art 18 Title 24 §§ 24-18-301, 24-18-302, 24-18-303, 24-18-304, 24-18-305, 24-18-306, 24-18-307, 24-18-308, & 24-18-309; add § 22-32-150; add § 22-30.5-529; add (5) § 18-5.5-102; amd (7)(h) § 24-30-1404; amd intro. & (5) § 24-37-101 (2022) (eff. July 1, 2023).

[9] American Data Privacy and Protection Act, A6319, 2023-2024 Legis. Sess. (N.Y. 2024) (Add Art 45 Title I §§1500 & 1501, Title II §§1510 – 1513, Title III §§1520 – 1529, Title IV §§1540 – 1544, Title V §§1550 – 1554, Gen Bus L; add §85 St Fin L); Digital Fairness Act, S2277, A3308, 2023-2024 Legis. Sess. (N.Y. 2024) (Add Art 39-FF §§899-cc – 899-ii, §350-a-1-, Gen Bus L; amd §292, add §296-e, Exec L; amd §§8 & 165, St Fin L; amd §814, Ed L); It's Your Data Act, S5555, 2023-2024 Legis. Sess. (N.Y. 2024) (Amd §§50 & 51, Civ Rts L; add Art 32-A §§676 – 676-q, Gen Bus L); New York Data Protection Act, S4201, A2587, 2023-2024 Legis. Sess. (N.Y. 2024) (Add Art 5-A §§81 – 89-b, Exec L); New York Privacy Act, S365, A3593, 2023-2024 Legis. Sess. (N.Y. 2024) (Add Art 42 §§1100 – 1107, Gen Bus L); S3162, A4374, 2023-2024 Legis. Sess. (N.Y. 2024) (Amd Art 39-F Art Head, add §899-cc, Gen Bus L; Add §99-m, St Fin L);

[10] California Consumer Privacy Act of 2018 & California Privacy Rights Act of 2020, Cal. Civ. Code §§ 1798.100, et seq. (operative Jan. 1, 2023); Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575, et seq. (eff. Jan. 1, 2023); Colorado Privacy Act, Colo. Rev. Stat. Ann. § 6-1-1301, et seq. (eff. July 1, 2023); Connecticut Data Privacy Act, Conn. Pub. Acts No. 22-15 (eff.

July 1, 2023); Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101, et seq. (eff. Dec. 12, 2023); owa Consumer Data Protection Act, Iowa Code § 715D.1 (eff. Jan. 1, 2025); Indiana Data Privacy Law, Senate Enrolled Act No. 5 (eff. Jan. 1, 2026).

[11] General Data Protection Regulation ((EU) 2016/679).

[12] General Data Protection Regulation, European Union (Withdrawal) Act 2018, as amd by Sched. 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulation 2019 (SI 2019/419).

Carter Ledyard & Milburn LLP uses Client Advisories to inform clients and other interested parties of noteworthy issues, decisions and legislation which may affect them or their businesses. A Client Advisory does not constitute legal advice or an opinion. This document was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. © 2023 Carter Ledyard & Milburn LLP.

related professionals

Matthew D. Dunn / Partner

D 212-238-8706

mdunn@clm.com

Jennifer "Jenny" Frank / Associate

D 212-238-8650

frank@clm.com

Jodutt Marwan Basrawi / Associate

D (212) 238-8767

basrawi@clm.com