wiley

NEWSLETTER

Biometrics Laws Are on the Books and More Are Coming: What You Need to Know

April 2019

Privacy in Focus®

A fingerprint, a retina scan, a voiceprint or facial scan – companies increasingly collect these and other biometric identifiers in the course of doing business, and the technology to collect and use them is developing rapidly. Policymakers and regulators from DC to state capitals have been grappling with whether and how to regulate the collection, use, and sharing of biometric identifiers, with the result that some laws are already on the books – and being actively enforced – while other states are considering similar laws. As companies increasingly turn to biometrics for purposes like improving security and convenience, they need to understand what privacy laws apply and what may be on the horizon.

Why is biometric privacy being regulated?

Although there is no agreed upon definition, in general, when policymakers and regulators discuss biometric data, they are concerned generally with data that is "biologically unique to [an] individual" and that is immutable.[1] As discussed below, different jurisdictions have defined biometrics in different ways for purposes of privacy laws.

The benefits of using biometric data can be extensive. One key example is using biometrics for authentication, which has security advantages over password-based authentication systems that are susceptible to a number of vulnerabilities.[2] As one observer has described – "[b]iometric authentication is simple for people to use and can streamline previously burdensome routine processes. These aspects, in combination with the difficulty it takes to mimic, make

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

biometric authentication an attractive asset to multiple industries."[3] Indeed, the government – at both the state and federal level – promotes the use of biometric data for authentication purposes. For example, in a 2016 report, the California Attorney General's Office specifically lamented password-based authentication systems and guided organizations to "protect access to critical systems and sensitive data" with multi-factor authentication, which "pairs 'something you know,' such as a password or PIN, with 'something you have,' ... or ***'something you are,' such as a biometric like a fingerprint."***[4] The federal government, including the National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC), also has promoted biometrics for increased security.[5]

Biometric data also allows for various efficiencies – from employee time-clocking to airport security. And the use of biometric data in the health care space is promising – "[b]iometric screening ... can help identify health risk factors ... improve health outcomes and decrease health disparities."[6]

At the same time, there are important privacy concerns regarding the collection and use of biometric data. One important concern is that biometric identifiers are immutable, and as a result, the stakes are high regarding any security breach. As the Illinois legislature explained in passing its biometric privacy bill: "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[7]

State laws

At the state level, there are a variety of ways that legislators are addressing biometric privacy, including through:

- ***Omnibus privacy laws***, like the California Consumer Privacy Act (CCPA)[8] that sweeps in biometric data in its broad definition of "personal information;"
- ***Biometrics privacy laws***, like those in Illinois,[9] Texas,[10] and Washington,[11] that create specific notice, consent, security, and other requirements for the collection, use, and sharing of biometric data; and
- ***Breach notification laws***, like those in Arizona,[12] Colorado,[13] Delaware,[14] Iowa,[15] Illinois,[16] Louisiana,[17] Maryland,[18] Nebraska,[19] New Mexico,[20] North Carolina,[21] Oregon,[22] South Dakota,[23] Wisconsin,[24] and Wyoming,[25] which all include biometric data as a data element that triggers notification requirements in the event of a data security breach.

These laws all treat biometric privacy and security in different ways. For example, just looking at the three biometric-specific laws, they differ in scope in important ways:

- **What data is covered?** Each law has its own variation on what data it covers, and how that covered data is defined. Illinois defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[26] The Illinois law also covers "biometric information," defined as

"any information, regardless of how it was captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[27] Washington defines "biometric identifier" to mean "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[28]

- **What uses of that data are covered?** State laws differ on this point as well. In Illinois, for example, obligations are triggered by merely being in possession of or collecting the covered data.[29] Washington's law, however, is not as broad in scope. That law generally imposes obligations for "enroll [ing] a biometric identifier in a database for a commercial purpose," and makes an explicit exception for uses of the data that are in furtherance of a security purpose.[30]
- **What type of notice and consent requirements does the law impose?** Each of the laws imposes notice and consent requirements, but they differ as well. In Illinois, notice and consent both need to be written.[31] Washington, on the other hand, makes clear that "[t]he exact notice and type of consent required to achieve compliance with [the notice and consent requirement] is context-dependent."[32]
- **Are there restrictions on transferring the data to a third party?** Texas, for example, restricts "[a] person who possesses a biometric identifier of an individual that is captured for a commercial purpose … [from] sell[ing], leas[ing], or otherwise disclos[ing] the biometric identifier" outside of a limited set of exceptions.[33]
- **Are there security requirements?** These laws generally require "reasonable" security requirements. In Washington, for example, a person in possession of biometric identifiers that have been enrolled for commercial purposes "[m]ust take reasonable care to guard against unauthorized access to and acquisition of" the data.[34] Companies should also be aware of data retention or deletion requirements. In Texas, for example, an entity covered by the law must "destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires."[35]
- **How is the law enforced?** The Illinois biometrics privacy law authorizes a private right of action for violations of the law; the biometrics laws in Washington and Texas do not.
- **Is there an exception for data covered under HIPAA?** The Illinois law, for example, excludes from the definition of "biometric identifier" "information captured from a patient in a health care setting or information collected, used, or stored for healthcare treatment, payment, or operations under [HIPAA]." [36]

And even looking beyond those three laws, the definition of covered "biometric" information varies widely from state to state. For example, California defines "biometric information" very broadly to include, among other things, "keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."[37]

In addition to the unique obligations that these laws impose on organizations that deal with biometric data, these laws also generate increased risk of liability. For example, the private right of action in Illinois's biometrics law has opened the door for plaintiffs' lawyers to file hundreds of cases.[38] And the Illinois

Supreme Court recently decided that under that law, there is no requirement to show actual harm, giving "its blessing to a flood of litigation, which may prove costly and deter companies from launching innovations in Illinois," as our colleagues have written.[39]

And the state laws that have already been enacted are not the end of the story. Several states are currently considering bills that address privacy concerns about biometrics – including biometric-specific privacy laws, as well as omnibus and state breach notification laws to include biometric data. For example, Florida is considering a biometrics privacy bill that models the Illinois law, complete with a private right of action.[40] California – a state that already has swept in biometric data under its omnibus privacy bill – is currently considering adding biometric data as an element of personal information under its state breach notification law.[41]

Federal efforts

At the federal level, Congress and multiple agencies have been working on privacy legislation and standards that would affect the collection and use of biometric information, among other types of data.

One area that has received particular attention is facial recognition. The Federal Trade Commission (FTC) has issued best practices that build upon the FTC's general privacy framework, which focuses on three main principles:

1. **Privacy by Design:** Companies should build in privacy at every stage of product development.
2. **Simplified Consumer Choice:** For practices that are not consistent with the context of a transaction or a consumer's relationship with a business, companies should provide consumers with choices at a relevant time and context.
3. **Transparency:** Companies should make information collection and use practices transparent.[42]

Additionally, the National Telecommunications and Information Administration (NTIA) has facilitated a multistakeholder process which developed a set of voluntary *Privacy Best Practice Recommendations for Commercial Facial Recognition Use*.[43] The principles highlighted by the NTIA document are transparency; developing good data management practices; use limitation; security safeguards; data quality; and problem resolution and redress.[44] And just like at the state level, there may be more to come in this Congress, bipartisan legislation on facial recognition – the Commercial Facial Recognition Privacy Act – is among the privacy proposals being considered.[45]

Moving Forward

The bottom line is that for companies dealing with biometric data – or those considering doing so – the landscape is complicated. There are evolving expectations and obligations, and growing liability risk. At the same time, the beneficial uses of this data – including for security use cases – are potentially enormous and have been encouraged in other contexts. It is critical for companies to be familiar with the current laws and guidance and pay attention to laws that may be on the horizon.

[1] *See* 740 ILCS § 14/5.

[2] Thomas B. Pahl, Acting Director, FTC Bureau of Consumer Protection*, Stick with Security: Require secure passwords and authentication*, FTC (Aug. 11, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication ("Consumers and employees often reuse usernames and passwords across different online accounts, making those credentials extremely valuable to remote attackers. Credentials are sold on the dark web and used to perpetrate credential stuffing attacks – a kind of attack in which hackers automatically, and on a large scale, input stolen usernames and passwords into popular internet sites to determine if any of them work. Some attackers time their log-in attempts to get around restrictions on unsuccessful log-ins. To combat credential stuffing attacks and other online assaults, companies should combine multiple authentication techniques for accounts with access to sensitive data.").

[3] Alexandro Pando, *Beyond Security: Biometrics Integration Into Everyday Life*, Forbes (Aug. 4, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#7884d07c431f.

[4] California Data Breach Report, 2012-2015, http://src.bna.com/cFY (emphasis added).

[5] *See, e.g., Protecting Personal Information: A Guide for Business,* Federal Trade Commission (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf ("The information could be further protected by requiring the use of a token, 'smart card,' thumb print, or other biometric—as well as a password—to access the central computer."); Ron Ross, et al., *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST 800-171 at D-10 (June 2015), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171.pdf (calling for the use of "multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.").

[6] Alexandro Pando, *Beyond Security: Biometrics Integration Into Everyday Life*, Forbes (Aug. 4, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#7884d07c431f.

[7] *See* 740 ILCS § 14/5.

[8] CCPA 1798.140(o)(1)(E).

[9] 740 ILCS § 14/.

[10] Tex. Bus. & Com. Code § 503.001.

[11] Wash. Rev. Code § 19.375.

[12] Ariz. Rev. Stat. § 18-551(11)(i).

[13] Colo. Rev. Stat. § 6-1-716(1)(a), (g).

[14] Del. Code tit. 6, § 12B-101(7).

[15] Iowa Code §§ 715C.1(11)(a)(5).

[16] 815 ILCS §§ 530/5.

[17] La. Rev. Stat. §§ 51:3073(4)(a)(v).

[18] Md. Code Com. Law §§ 14-3501(e)(1)(i)(6).

[19] Neb. Rev. Stat. §§ 87-802(5).

[20] N. M. S. A. 1978, § 57-12C-2(A), (C).

[21] N.C. Gen. Stat §§ 75-61, 14-113.20(b).

[22] Oregon Rev. Stat. §§ 646A.602(11).

[23] S.D. Cod. Laws §§ 22-40-19(4).

[24] Wis. Stat. § 134.98(b).

[25] Wyo. Stat. § 6-3-901(b).

[26] 740 ILCS § 14/10. Texas has a near-identical definition: "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." Tex. Bus. & Com. Code § 503.001(a).

[27] 740 ILCS § 14/10.

[28] Wash. Rev. Code § 19.375.010(1).

[29] 740 ILCS § 14/15.

[30] Wash. Rev. Code § 19.375.020(1).

[31] 740 ILCS § 14/15(b).

[32] Wash. Rev. Code § 19.375.020(2).

[33] Tex. Bus. & Com. Code § 503.001(c)(1).

[34] Wash. Rev. Code § 19.375.020(4)(a). *See also* Tex. Bus. & Com. Code § 503.001(c)(2) ("A person who possesses a biometric identifier of an individual that is captured for a commercial purpose ... shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other

confidential information the person possesses.").

[35] Tex. Bus. & Com. Code § 503.001(c)(3) (includes exceptions).

[36] 740 ILCS § 14/10.

[37] CCPA 1798.140(b).

[38] *See* Ben Koch, *Ill. High Court Sides With Consumers in Biometric Privacy Suit*, Law360 (Jan. 25, 2019), https://www.law360.com/appellate/articles/1122073.

[39] Megan Brown and Boyd Garriott, *Illinois: Actual Injury Not Required for Privacy Lawsuit; Inviting Costly Litigation against Innovators*, Wiley Connect (Jan. 25, 2019), https://www.wileyconnect.com/home/2019/1/25/illinois-actual-injury-not-required-for-privacy-lawsuit-inviting-costly-litigation-against-innovators.

[40] Jessica Davis, *Florida Proposes State Biometric Data Privacy Legislation*, Health IT Security (Mar. 11, 2019), https://healthitsecurity.com/news/florida-proposes-state-biometric-data-privacy-legislation.

[41] See California AB 1130, http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130.

[42] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[43]*Privacy Best Practice Recommendations For Commercial Facial Recognition Use*, NTIA, https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf.

[44] *Id.*

[45] *See* S. 847, 116th Cong. (in progress 2019-2020).