Biometric Data: Companies Should Act to Mitigate Risks in the Face of Growing Regulations and Increased Risk for Liability

Date: 06 / 03 / 19
Publication: M&S Industry Alert
Related to:
There is a growing trend to regulate biometric data and severely punish companies that do not adequately protect this data. Every company that collects or uses biometric data should be careful to ensure compliance with applicable laws intended to protect this sensitive information.

**What is Biometric Data?**

Biometric data is generally defined as ‘unique physical identifiers including fingerprints, facial structures, iris scans, and voiceprints.’ While there are no current Federal laws governing the collection, use, and protection of biometric data, several states do specifically regulate this most sensitive data.

**Much More than Just HIPAA**

When considering risk related to protecting personal information, we tend to focus on personally identifiable health information protected under HIPAA, or requirements related to protecting sensitive information in the finance industry under the Gramm-Leach-Bliley Act. However, tech-savvy companies in virtually every industry have been using biometric information for years, and increased use and storage of this type of information is gaining in popularity. This increased use is largely because these unique physical identifiers are believed to offer greater security than alphanumeric passwords or other traditional security measures that can be easily faked or stolen.

Companies are finding that use of biometric information can be an advantageous business tool, both because of the security protections and as biometric applications create operational efficiencies. Particularly in the health care industry, companies have been quick to broadly embrace the use of biometric identifiers in their operations. For example, large hospital systems in Texas and New York now use palm screening tools for patient intake to streamline administrative processes, avoid patient confusion, and cut down on burdensome paperwork. In addition, health care apps continue to be developed by tech entrepreneurs which track, store and transmit biometric information to providers for more efficient patient treatments.
The collection, use and storage of biometric identifiers, however, carry substantial legal risk. Physical attributes that make up biometric information are difficult to replicate and, therefore, offer tremendous value for cybersecurity criminals. In addition, the damage to a consumer caused by theft, leakage or loss of biometric information can be substantial—more so than a stolen password that can be easily altered or changed. As a result, new laws are being introduced and passed throughout the country to regulate this area, and applicable corporations should be vigilant in monitoring statutes, regulations and proposed legislation and adjusting policies and procedures accordingly.

**Where is Biometric Data Regulated?**

Currently, only Illinois, Washington and Texas have statutes specifically devoted to the protection of biometric information. Illinois, in particular, has become a litigation lightning rod for corporations who collect, store and use biometric information. The Illinois Biometric Information Privacy Act ("BIPA") is unique because it allows for a private cause of action. Earlier this year, this risk for liability under the law significantly increased when the Illinois Supreme Court held that plaintiffs are not required to allege actual injury to collect damages, seek injunctive relief and obtain attorneys' fees under the law. *See Rosenbach v. Six Flags Entertainment Corp.*, ___ N.E.3d __, 2019 W.L. 323902 (Ill. Jan. 25, 2019). In the Rosenbach case, the Court allowed for damages against Six Flags because it did not provide specific statutory disclosures related to its collection and use of biometric data it obtained from customers, even though the plaintiffs made no assertion that the data had in any way been misappropriated or misused, or that they had incurred any losses. Accordingly, violations of BIPA are essentially strict liability offenses. The private right of action makes violations particularly appealing in the class action context and companies should anticipate increased scrutiny of corporate policies and procedures related to biometric data they possess.

Other states have incorporated biometric information protections into larger consumer protection laws. For example, the California Consumer Privacy Act ("CCPA"), effective January 1, 2020, provides individuals with certain rights regarding their personal information, which includes by definition biometric data. Under CCPA, individuals may obtain their own personal information stored by companies, prohibit
its use or disclosure, and require companies to delete it on demand. In addition, companies storing personal information must implement strict security and protection protocols under the CCPA, and could face lawsuits from the California attorney general for potential violations.

Several other jurisdictions including Arizona, Colorado, Delaware, Georgia, Iowa, Louisiana, Massachusetts, Nebraska, New Mexico, New York, Maryland, Massachusetts, Vermont, Wisconsin, Wyoming, and Vermont include biometric information in definitions of protected information for their respective data breach notification laws. In addition, several state legislatures are actively seeking to pass laws specifically related to biometric data privacy and have seen the introduction of related bills in 2019 legislative sessions.

The United States Congress also is focusing on this issue with the introduction of SB 847, the Commercial Facial Recognition Privacy Act of 2019 (“CFRPA”), earlier this year which currently is sitting in the Senate Commerce Committee. CFRPA would prohibit commercial users of facial recognition technology from collecting and re-sharing data for identifying or tracking consumers without the consumer’s consent; require companies to notify consumers when facial recognition technology is being used; and require third-party testing and human review of facial recognition technologies prior to their implementation in an effort to address concerns related to inaccuracy and bias that could cause harm to consumers.

Companies that collect, store or use biometric data and conduct business internationally may also be subject to foreign requirements. The General Data Protection Regulation (“GDPR”) applies to entities that conduct business in any of the 28 European Union countries—or hold personal data of any E.U. residents—and strictly prohibits processing of (i.e. disclosing to third parties) E.U. citizens’ personal data, including biometric information, unless exceptions apply such as explicit consent. Storage and safeguard requirements also apply under GDPR and penalties for violations include steep fines of up to 20 million Euros. Of interest, the GDPR definition of biometric information is expansive and includes behavioral characteristics such as habits or actions as well as physical or physiological attributes.
As noted above, current and pending laws related to biometric information are complex and vary greatly from state to state and outside the United States. As new legislation continues to be introduced and considered, the risks for companies that collect or use biometric information will continue to increase. In order to promote compliance with applicable laws while taking advantage of this important and rapidly developing technology, businesses that collect, store, use, or otherwise access biometric information should be aware of all relevant guardrails and potential for liability, and take steps to implement policies and procedures that, at a minimum, meet the applicable statutory requirements.

This alert was written by Robert Wells, Michele Cohen, Veronica Jackson and Christopher Tully, lawyers in the Baltimore office at Miles & Stockbridge.

Any opinions expressed and any legal positions asserted in the article are those of the author(s) and do not necessarily reflect the opinions or positions of Miles & Stockbridge P.C. or its other lawyers. This article is for general information purposes and is not intended to be and should not be taken as legal advice on any particular matter. It is not intended to and does not create any attorney-client relationship. Because legal advice must vary with individual circumstances, do not act or refrain from acting on the basis of this article without consulting professional legal counsel. If you would like additional information on the subject matter of this article, please feel free to contact any of the lawyers listed above. If you communicate with us, whether through email or other means, your communication does not establish an attorney-client relationship with either Miles & Stockbridge P.C. or any of the firm’s lawyers. At Miles & Stockbridge P.C., an attorney-client relationship can be formed only by personal contact with an individual lawyer, not by email, and requires our agreement to act as your legal counsel together with your execution of a written engagement agreement with Miles & Stockbridge P.C.