Realize the risk

Biometric data could widen your exposure if you're not cautious

LUCAS BLOWER
Attorney at Law
Brouse McDowell

(330) 434-7114
lblower@brouse.com

AMANDA PARKER
Attorney at Law
Brouse McDowell

(330) 535-5711
aparker@brouse.com

WEBSITE: To learn more about how biometric data could create liability for your business, visit www.brouse.com.

Insights Legal Affairs is brought to you by **Brouse McDowell**

Seeking to reduce their risks and improve security, business owners may unknowingly take steps that invite more risk of liability. Upgrading your security by using biometric data to strengthen security protocols can subject your business to liability from an increased risk of privacy litigation. More businesses are using biometric data for internal operational security, consumer authentication and other identification purposes.

While there is no uniform definition, biometric data is information derived from human biological and behavioral characteristics such as fingerprints, facial scans and voiceprints. Today, the use of biometric data in everyday interactions is exploding — retailers are using fingerprint scans at the point of sale to verify customer payment, banks have announced plans to replace PIN numbers with facial and retina scans at ATMs, and employers are increasingly using biometric identifiers to access and maintain data centers.

Smart Business spoke with Lucas Blower and Amanda Parker, Attorneys at Law at Brouse McDowell, about the consumer and employee privacy implications of this trend.

How is biometric data governed?

One problem with biometric data is that currently, there is no federal or uniform law that directly addresses its collection and use. Consequently, it is unclear whether biometric data will be treated as Personal Identifiable Information or if it will be subject to a heightened standard. While there are regulations for the health care, insurance and employment context, these laws do not address novel uses businesses may employ using biometric data. In some instances, biometric data may be subject to the Health Insurance Portability and Accountability Act or the Genetic Information Nondiscrimination Act.

Currently, the only states with pending or existing laws addressing biometric data are Illinois, Texas, Alaska, California, New York and Washington. The legislation in these states often addresses requirements such as notice, consent, disclosure, policy and destruction periods. Several such laws also provide for civil penalties for each violation.

Additionally, the Federal Trade Commission may have the authority under the Federal Trade Commission Act to pursue enforcement action where businesses do not comply with their own policies regarding consumer data collection. This inconsistent treatment of biometric data increases the potential risk of litigation for businesses using biometric identifiers.

What other issues should be considered when using biometric identifiers?

Businesses across industries collect, use, protect and share biometric data differently. As a result, there are no clear standards for how companies should handle biometric data. Decisions on how to collect, store, protect, share and analyze biometric data should be made in consideration of existing and emerging privacy laws, but also in light of available insurance coverage. Whether businesses use biometric data to prevent fraud, increase internal controls or promote wellness, the collection of biometric data increases a company's exposure to a data breach. Having adequate coverage in the event of a data breach is the only way to protect against the cost of litigating privacy claims and to reduce the risks associated with using biometric data. A company's policies and controls for handling biometric data can also affect whether a data breach is covered or excluded from coverage. Insurance companies are adding new exclusions, especially those applying to cyberrisks. Businesses that fail to follow minimum required practices will likely find themselves without coverage.

How can I minimize the risks?

In order to ensure your biometric technology is reducing risk and not increasing your exposure, businesses should develop thorough policies and controls for handling biometric data. Additionally, businesses must develop and train employees in compliance with their privacy and data security policies. Finally, by periodically auditing and re-evaluating both your privacy and data security policies and employee compliance, businesses can reduce the risks of using biometric data and ensure that they won't be denied coverage in the event of a data breach for failure to follow minimum required practices. ●

© 2016 Smart Business Network Inc. Reprinted from the July 2016 issue of *Smart Business Cleveland*.