Volume 2, No. 6 | November–December 2019

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 2, No. 6 | November–December 2019

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

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

Robert A. Wells, Veronica D. Jackson, and Christopher J. Tully*

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. The authors of this article discuss biometric data and advise businesses that collect, store, use, or otherwise access biometric information to be aware of all relevant guidance and potential for liability, and take steps to implement policies and procedures that, at a minimum, meet the applicable statutory requirements.

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

Robotics, Artificial Intelligence & Law / November–December 2019, Vol. 2, No. 6, pp. 415–419.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

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 healthcare 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, healthcare apps continue to be developed by tech entrepreneurs who 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 cybercriminals. 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 that 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.[1] In *Rosenbach v. Six Flags Entertainment Corp.*, 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 that store 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[2] 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 U.S. 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 EU countries—or hold personal data of any EU residents—and strictly prohibits processing of (i.e., disclosing to third parties) EU 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.

Conclusion

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 guidance and potential for liability, and take steps to implement policies and procedures that, at a minimum, meet the applicable statutory requirements.

Notes

* Robert A. Wells is a principal in the law firm Miles & Stockbridge P.C. focusing on healthcare regulatory and corporate matters, representing both long-established and start-up healthcare companies. Veronica D. Jackson is counsel at the firm, practicing in the area of data privacy and security, and assisting clients with both preventive efforts as well managing compliance issues in the aftermath of a data breach. Christopher J. Tully is an associate at the firm with broad-based transactional, regulatory, and litigation healthcare practice. The authors may be reached at rwells@milesstockbridge.com, vjackson@milesstockbridge.com, and ctully@milesstockbridge.com, respectively.

1. *See Rosenbach v. Six Flags Entertainment Corp.*, ___ N.E.3d ___, 2019 W.L. 323902 (Ill. Jan. 25, 2019).

2. Arizona, Colorado, Delaware, Georgia, Iowa, Louisiana, Massachusetts, Nebraska, New Mexico, New York, Maryland, Massachusetts, Vermont, Wisconsin, Wyoming, and Vermont.