Volume 5, No. 2 | March–April 2022

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 5, No. 2 | March–April 2022

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
Production Editor: 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 inquiries 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, 631.291.5541.

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 contact:

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 8 a.m.–8 p.m. 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)

From Fingerprints to Facial Recognition: Scanning Developments in Biometric Technology

Jeffrey N. Rosenthal, David J. Oberly, and Amanda M. Noonan*

The landscape of biometric technology is rapidly evolving. In recent years, new and exciting biometric products, businesses, and service providers have entered the market. As a result, tools that were once pure science fiction have morphed into mundane aspects of modern life. Biometric technology itself is becoming a staple of business and consumer use alike. As the implementation of biometric technology spreads farther and wider, the impact of its regulation—and potential for class action litigation exposure—is already evident. Household names like Facebook, Shutterfly, TikTok, Walmart (and others) have entered into multi-million-dollar settlements to resolve biometric class actions. This article discusses existing/developing biometric technologies, the legal landscape, notable settlements, and provides practical guidance for companies using—or considering the use of—biometric technology.

Biometric technology is all around us. Whether clocking into work by scanning your fingerprint, unlocking a cellphone with your face, or virtually "trying on" a product via your smartphone camera, biometric technology is, quite literally, at our fingertips.

The reach of biometrics will only expand with new innovations. Even now, the prevalence of biometrics can be seen across the banking, technology, travel, healthcare, entertainment, and security industries. The marketplace for biometric technology has already grown to over $20 billion dollars annually; it is expected to reach close to $60 billion by 2025.

As biometric technology gains a global foothold, it is important to not only understand how biometric technology is used in the worldwide marketplace but also what it is and what it does.

At its core, biometric technology is used to identify a person or verify their identity through their unique physical characteristics that can be used for automated recognition. Biometric technology arises in many forms, including now-common fingerprint scanning and facial recognition technologies, all the way to iris and retina

Robotics, Artificial Intelligence & Law / March–April 2022, Vol. 5, No. 2, pp. 123–128.

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

scanning and voice recognition. Despite their obvious differences, the crux of all these biometric technologies involve capturing an individual's unique biometric identifiers, typically for the purposes of identification and verification.

Biometric Technology Overview

Perhaps the most well-recognized biometric technology is facial recognition. Facial recognition technology uses biometrics to "map" facial features and produce a unique code or "faceprint" that can be used to identify or verify an individual. In this way, facial recognition technology reads the unique geometry of an individual face—including, for example, eye socket depth, bone features, contours, and distance between facial landmarks (nose, mouth, lips, eyebrows, etc.).

Biometric technology also includes fingerprint, iris, and retina as well as audio recognition. Like facial recognition technology, in its other forms, biometric technology similarly operates to capture unique biometric features that serve individual identification/verification purposes.

For instance, fingerprint scanning technology creates digital images of a fingerprint to document its patterns and ridges. Iris scanning can generate mathematical formulas for pattern recognition of the iris of a human eye. Similarly, retina scanning captures a retinal image to compare unique features of retinal blood vessels. And auditory recognition involves identifying and capturing an individual's "voice print"—the unique characteristics of an individual's speech pattern.

Biometric technologies are vast and continue to develop, including vein recognition, gait recognition, heart rate recognition, and others.

Biometric Technology Implementation Across Industries

Biometric technology is readily accessible and used broadly by businesses and technology platforms. Below are some of the different types of biometric technologies currently implemented across various industries.

Authentication Technology

Authentication technology is a staple of the biometric industry and is utilized by many platforms. It does exactly what biometric technology is designed to do—verify user identities, most commonly, for security purposes. Multiple forms of biometric technology—facial recognition, fingerprint scanning, audio recognition, and iris scanning, as examples—can be used to accomplish this objective. Authentication technology is typically used to gain access to both physical and digital resources, including cell phones and digital devices, as well as workplaces and other physical spaces.

Authentication technology currently has the widest reach through its broad use in personal digital devices. Millions of users rely on authentication technology to unlock their cell phones. Starting with fingerprint recognition—and now more commonly facial recognition—biometrics is what allows secure and convenient access to their personal digital devices. Simply putting your thumb on a device's sensor, or showing your face within view of a camera, is all that is required to gain access. The biometric technology then compares the individual's biometric features with those biometric identifiers previously stored by the technology. In practice, the authentication process is instantaneous.

Aside from digital devices, both fingerprint scanning and facial recognition technology are often used by businesses to gain access to physical spaces or records. For example, employers often utilize these forms of biometrics to allow entry into a physical premise and as a means of tracking employee time. Similarly, the healthcare industry is increasingly relying on biometric authentication for patient identification. This industry often turns to the most secure forms of biometric authentication—iris and retina scanning—to securely identify patients through high contrast photographs of an individual's iris or retina to capture their unique biometric identifiers.

Biometric authentication technology, while coming in many forms and utilized for varying purposes, offers convenient, efficient, and secure methods to authenticate individual's identity. It is expected that biometric authentication technology will only grow and continue to be relied on for identity verification purposes.

Photo Tagging/Matching Technology

Photo tagging is another form of facial recognition technology that has gained widespread traction. Most frequently used by personal digital devices and social media platforms, photo tagging uses facial recognition technology to identify and organize photographs by individual faces. The process involves obtaining an image of a face on an uploaded photograph, capturing data of that individual's unique biometric facial features (much like with authentication technology), and matching the image to existing photographs to identify which images belong to the same person.

Tech giants have employed photo tagging technology on their platforms with high levels of accuracy. For instance, when Facebook implemented its photo tagging technology it matched photographs belonging to the same person with an accuracy rate of 97.25 percent. Google's "Google Photos" technology reached 99.63 percent accuracy on its own photo tagging technology. Both reach massive numbers of users and have transformed social media and digital photo marketplace. Once uploaded to either of these platforms, or others utilizing this same technology, photos uploaded by the user itself and others are matched and easily organized to group photos of the same individual together.

It is not only the social media and technology industry that has implemented this type of photo matching facial recognition technology. It has become increasingly relied on by law enforcement and security agencies in their identification efforts. Following the same process, law enforcement agencies have implemented this technology by comparing photographs to an accumulated database to match identities related to their investigations. The magnitude of this effort is evident—a 2016 study found that almost half of American adults are in a law enforcement facial recognition database. Even Amazon has jumped in, promoting its own technology to law enforcement that can recognize up to 100 people in a single image and match those against databases containing hundreds of millions of faces. Biometric photo matching technology has the potential to revolutionize law enforcement investigative practice.

Legal Landscape

The breadth and accessibility of biometric technology across almost all industries cannot be understated. Despite its

sophistication, biometric technology is easy to use, readily available, and currently utilized by millions of individuals, businesses, and agencies daily.

The broad reach of biometric technology, however, has spurned privacy concerns. As a result, regulations have been implemented at the state and municipal levels to govern the use and development of this technology. Only three states—Illinois, Texas, and Washington—have enacted targeted laws directly regulating the collection and use of biometric data. But even with relatively few laws currently on the books, class action litigation has exploded. Indeed, companies that are at the forefront of implementing biometric technology have been targeted for bet-the-company litigation with massive financial consequences.

Notable cases have reached astronomical settlements resulting from purported biometric privacy violations. This includes Facebook, which was sued for alleged violations of Illinois biometric privacy law resulting from its photo tagging technology. In that case, Facebook reached a $650 million settlement with approximately 1.6 million putative class members. In a similar vein, social media giant TikTok reached a $92 million settlement with putative class members in a case pending before an Illinois district court for alleged biometric privacy violations. Companies ranging from Shutterfly, Six Flags, to Top Golf have paid, or agreed to pay, million-dollar settlement figures to resolve biometric privacy litigation. In many more cases, biometric technology litigation is ongoing—and its financial impact is yet undetermined. But what *is* certain is that as regulations at every level continue to develop, the legal consequences of biometric technology law will be at the forefront of its continued use and development.

Conclusion

Biometric technology is present in virtually every industry, adding convenience, security, and efficiency to providers and users. Such technology will only increase as the technology continues to evolve and innovations are expanded on across the corporate, government, and private sectors. Regulation of biometric technology too will continue to expand. The ultimate regulatory and financial ramifications of biometric privacy law will be a key development in biometric technology's evolution.

Note

* Jeffrey N. Rosenthal is a partner in the Philadelphia office of Blank Rome LLP where he leads the firm's Biometric Privacy Team and is a member of its Privacy Class Action Defense and Cybersecurity & Data Privacy groups. David J. Oberly is an attorney in the firm's Cincinnati office and is a member of its Biometric Privacy, Privacy, Security & Data Protection, and Privacy Class Action Litigation groups. Amanda M. Noonan is an attorney in the firm's Chicago office and is a member of the firm's Biometric Privacy Team and General Litigation Group. The authors may be reached at jeffrey.rosenthal@blankrome.com, david.oberly@blankrome.com, and amanda.noonan@blankrome.com, respectively.