Volume 4, No. 2 | March–April 2021

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 4, No. 2 | March–April 2021

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 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, 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 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)

How the Use of Biometrics Is Affecting the Air Transportation Industry

Elaine D. Solomon*

Biometrics are unique physiological and behavioral identifiers that include such things as fingerprints, facial recognition, iris and retina scans, and voice and speech recognition. With respect to kick-starting air travel, which has been severely limited due to COVID-19, one key may be expanding the use of biometrics to restore passenger confidence in a secure, efficient, and healthy passenger experience. The author of this article discusses biometrics and air travel.

The increased use of biometrics will continue to have a profound effect on the air transportation industry, and the COVID-19 pandemic is fueling the need to accelerate that implementation. There has been a lot of discussion lately about needing to balance the need for containment of the virus versus restarting the economy. Yet the question is how to accomplish both of those goals. With respect to kick-starting air travel, one key may be expanding the use of biometrics to restore passenger confidence in a secure, efficient, and healthy passenger experience.

An Overview of Biometrics

Biometrics are unique physiological and behavioral identifiers that include such things as fingerprints, facial recognition, iris and retina scans, and voice and speech recognition. Common examples of currently used biometric technology are our use of fingerprints and/or facial recognition to unlock cell phones and laptops.

Types of Biometrics

Fingerprints

Historically, fingerprints have been used for criminal investigation purposes. With respect to the aviation industry, biometrics

Robotics, Artificial Intelligence & Law / March–April 2021, Vol. 4, No. 2, pp. 105–114.

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

are used by such entities as U.S. Customs and Border Protection ("CBP") to control international border entry points. The features of a fingerprint (such as ridges) are extracted and a biometric template is created. Another associated biometric is palm and hand recognition. Palm recognition is similar to fingerprint recognition, in that certain physiological elements such as ridge and valley patterns are utilized to create a biometric template, which is then processed via an algorithm and stored in a database as the individual's biometric template. Hand geometry has been in use for quite some time (dating back to the 1970s). As an example, hand geometry can be used to grant access to facilities. The downside to this biometric technology is that it changes over time as a person ages.

Vein Patterns in Hands and Fingers

Vein patterns can be captured via infrared light. The upside of this type of biometrics is that it is relatively stable over a person's lifetime. A related biometric technology is the use of infrared thermograms to recognize heat radiation patterns in faces or hands.

Facial Recognition

Facial recognition is a well-known biometric used by such entities as the Federal Bureau of Investigation and law enforcement agencies. Ear recognition is another biometric technology in which distinctive features of the ear (such as shape) can be analyzed. Both faces and ears can be analyzed, and then algorithms used, to create a biometric template for identity authentication. Facial recognition will continue to be the most widely used methodology for biometric identity verification, and artificial intelligence will be utilized to determine if a "live" face is being used versus a mask or an artificial intelligence–based image of a face.

Eyes, Including Iris and Retina Recognition

Facial and iris recognition have been widely considered with respect to air traveler check-in, bag-drop, and boarding processes. The iris is considered to be one of the most accurate biometric characteristics because it has many distinguishing characteristics. In addition, the retina has distinctive features that are difficult to replicate and, because of that, retina scanning has historically been used for military applications.

Gait

The way a person walks can also be used as a biometric indicator, with algorithms being used to analyze an individual's gait features. The downside of this indicator is that it can be affected by such things as walking surface, injury, and footwear.

Voice

Biometric voice analysis utilizes voice recognition software, where an individual needs to repeat several phrases or words to enable the software to have enough data to create a voice print template. The downside of this biometric technology is that it can be affected by age, physical condition, and background noise.

Data Privacy

Biometric data is generally stored either locally (i.e., in an individual's device, such as a cell phone), in a centralized server (stored in the United States or abroad), or in a multi-location data location. Generally, the biometric data is gathered and then an algorithm is applied to convert the data into a numeric representation that is then used as the biometric template, which is then used to compare data.

The Overall Regulatory and Legal Scheme

The States

Some states (including Illinois, Washington, and Texas) have laws addressing biometrics. Illinois has the Biometric Information Privacy Act ("BIPA"), which, unlike other laws, allows for a private cause of action. Further, the Illinois Supreme Court has held that plaintiffs in cases allegedly arising under BIPA do not have to allege actual injury to collect damages, attorneys' fees, or to seek injunctive relief.[1] In *Rosenbach*, the court allowed the plaintiffs to seek damages against Six Flags even though the plaintiffs did not allege that the data had been misused or misappropriated, or that the plaintiffs had in fact incurred any actual damages. Because of the scope of the BIPA, it has been viewed as a favorite vehicle for class action lawsuits.

In other states, biometric-based causes of action are encompassed within state consumer protection laws, including, as examples, the following:

- In California, the Consumer Privacy Act ("CCPA") was effective as of January 1, 2020. The CCPA affords individuals certain protections regarding personal information (defined to include biometric data). Under the CCPA, an individual can prohibit use or disclosure of personal information, and it also requires companies to delete such information on demand. Companies storing such information must also put in place protection and security safeguards, and failure to do so may result in possible liability for violation of the CCPA.
- Other states such as Arizona, Colorado, Delaware, Georgia, Iowa, Louisiana, Massachusetts, Nebraska, New Mexico, New York, Maryland, Massachusetts, Vermont, Wisconsin, Wyoming, and Vermont include biometric information in their definition of protected information with respect to their data breach notice laws. Thus, lawsuits for alleged biometric violations may be encompassed within these state consumer protection laws.

The Federal Government

The use of biometrics in the air transportation industry increased dramatically after the 9/11 terrorist attacks. The result was creation of the Department of Homeland Security ("DHS"), Customs and Border Protection ("CBP"), and the Transportation Security Administration ("TSA"). Certain federal legislation required the use of biometrics for the United States Exit-Entry program for international travelers (now called Biometric Entry-Exit), and authorized the TSA to use biometrics for passenger screening. Those laws include The Enhanced Border Security and Visa Entry Reform Act of 2002,[2] The Intelligence Reform and Terrorism Prevention Act of 2004,[3] and The Implementing Recommendations of the 9/11 Commission Act of 2007.[4]

The TSA began testing biometric solutions in 2015 to improve aviation security by modernizing aviation passenger identity verification through the use of biometrics instead of manual and paper-based identity verification processes. The TSA's "roadmap"

concerning implementation of biometrics has identified certain objectives and guiding principles to enhance aviation security, streamline operations, simplify the user experience, address privacy issues (including errors related to race, gender, or age), and assess cybersecurity issues. The TSA states that the primary means of identity verification for aviation security screening will remain the use of facial images, whereas use of fingerprints will continue to serve as the primary biometric modality for trusted traveler and other credentialed enrollments.

The TSA will partner with CBP regarding the use of biometrics for international travelers, both to determine the feasibility of this goal and to develop inter-agency policies and procedures to ultimately simplify and streamline operations. Over the years, CBP has invested significant resources in developing a Biometric Air Exit capability to fulfill federal government mandates to biometrically verify the departure of foreign nationals from the United States. In 2017, CBP made the critically important decision to use facial recognition for future operations rather than traditional fingerprinting. Sharing of existing CBD databases (such as "facial galleries" available through the Department of State U.S. passport and visa photos) and technology will facilitate data exchange and operational coordination between CBD and TSA.

The next goal is to utilize biometrics for TSA Pre-Check passengers, which will require updating of TSA Pre-Check databases to modernize the passenger experience. This includes the use of passport photos that are on file, and other voluntary opt-in approaches.

Another TSA goal is to expand biometrics usage for all domestic travelers, including the use of existing and available traveler data.

The TSA also states the goal of developing a supporting infrastructure for biometric solutions, which will involve working with the DHS and aviation industry partners to set standards, coordinate legal and strategic policies, and make sure issues are resolved in a consistent and coordinated manner.[5]

International

For EU countries, the General Data Protection Regulation ("GDPR") applies to any entities that conduct business in the EU countries, or data with respect to any EU residents. The GDPR prohibits disclosing EU citizens' personal data to third parties.

The personal data within the ambit of the GDPR encompasses biometric data. GDPR also includes certain safeguards and storage requirements for biometric data, and there are penalties for violation. The GDPR goes well beyond what is encompassed within U.S. biometrics laws, to include behavioral characteristics such as physical or physiological characteristics.

Biometrics Goals

The goal regarding increased use of biometrics in the air transportation industry is to achieve a seamless travel experience, so passengers can use a single biometric identity verification "token" (such as face, fingerprint, iris, or other biometric indicators) when traveling through an airport—from check-in through to bag-drop, security, a business lounge, boarding a flight, and usage at the destination airport. Perhaps biometrics will even be used to pay for your purchases at airport shops and for in-flight purchases with just a look at a camera.

The hope is that biometrics will improve the economics of air travel by improving the efficiency of airport operations and increasing passengers' free time at the airport to make purchases and relax. Passengers will no longer need to find and show their driver's license, passport, visa, boarding pass, or other paper-based forms of identification. The "self-service" airport experience will include everything from enrolling in the program, flight check-in, boarding pass, bag tag, automatic bag drop, pre-security immigration analysis, security screening, business lounge access, and self-boarding your aircraft. As an example, self-service bag-drop kiosks use facial recognition technology to match a passenger with his or her tickets and baggage. One simple facial scan can create a unique biometric key for each passenger that can then facilitate a seamless air travel experience and enhance aviation efficiency and security.

The Effect of COVID-19 on the Aviation Industry

COVID-19 has struck a devastating blow to the travel and air transportation industry. Those industries must implement contactless systems that will make passengers once again feel comfortable flying without fear of health risks. The air transportation industry

needs to regain passengers' confidence that they can travel by air without jeopardizing their health and safety.

The increased use of biometrics to enhance "touchless" technology (such as facial recognition and contactless fingerprints) will facilitate that goal. The benefits will be felt not only by travelers but also by airlines and airport personnel whose possible exposure to the virus will be lessened. Reducing or eliminating the use and exchange of paper documents for identity verification will notably decrease the risk of transmitting the virus. The goal is to create touchless checkpoints throughout the airport so that the air travel experience becomes quick, hygienic, and secure.

In light of the pandemic, there is also a need to avoid crowding and queuing (which will facilitate better social distancing) in order to avoid face-to-face and human-to-machine interactions, avoid the use and exchange of paper travel documents during the air travel experience, and to introduce rapid COVID-19 health screening at airports so passengers can comply with the ever-changing travel restrictions imposed by states and countries. Indeed, some airlines such as United and Spirit have already started offering COVID-19 testing at certain airports. Foreign air carriers such as Emirates have also launched a contactless airport experience (using a combination of facial and iris recognition) for passengers traveling from or through Dubai. Biometrics will also be used for COVID-19 contact tracing, and thermal scanning can be used at airport touchpoints to detect if a passenger has an elevated body temperature, which is a common sign of illness.

The use of biometrics is necessary not only to address health concerns but also to provide significant business and economic benefits. Notably, biometrics can increase efficiency and improve cost margins; travel for business or pleasure stimulates the economy at both originating and destination locales; decreased wait times at the airport will benefit airport shops, restaurants, and other retailers in the form of increased revenues, as well as reduce staff and overall expenses; and decreased boarding times will lessen flight delays, which cost airlines billions of dollars per year. The concomitant building or rebuilding of infrastructure to support the use of touchless biometric technologies at airports and throughout the travel industry will also facilitate economic growth. To achieve this goal, TSA and other government and industry partners must work with airlines and airports to address these issues. The benefits

of biometrics in the air transportation industry will last well past the time that the COVID-19 pandemic ends.

Airports and Airlines Using Biometrics

Some airlines and airports are already on the forefront of biometrics usage. As an example, Delta was one of the first American air carriers to use biometrics at Atlanta's Hartsfield-Jackson International Airport. Passengers traveling through the international terminal can opt-in to use an end-to-end seamless airport experience in certain parts of the airport if he or she agrees to use face recognition technology, including use of facial recognition technology for check-in, bag drop-off, security screening, and flight boarding. Use of the CBP database facilitates passenger identification for this voluntary program.

At Seattle-Tacoma International Airport ("Sea-Tac"), facial recognition biometrics based upon images previously collected by CBP for passport or visa application are being used for a Biometric Air Exit program for international passengers departing Sea-Tac. Passengers have the right to opt out of this biometric processing. Wishing to control certain privacy-related issues (such as unauthorized commercial use of facial images, data security, unintended image capturing, and cultural sensitivity), the local Port of Seattle Commission owns and controls this program rather than the federal government.

Denver International Airport has launched a program to use biometrics to implement touchless technology throughout the airport. The goal is to create a touchless environment, maximize social distancing, and assess health risks as travelers move through the airport.

The Debate Over the Increased Use of Biometrics

Although the benefits of biometrics usage in the air transportation industry are arguable outweighed by any possible concerns, some issues have been raised. As an example, some have argued that increased use of biometrics may create a goldmine of information and data for cybercriminals, and also result in increased identity theft. If biometric data is locally stored and then the device (for example, a cell phone) is stolen, then the data is compromised. Even

if such data is stored on a server, it could be subject to cybersecurity attacks and breaches. Fears of invasion of privacy and heading into a "surveillance society" are other concerns, as well as an allegation that facial recognition is biased against women, individuals of color, and the elderly. Further, the algorithms used for facial recognition are not 100 percent accurate. Individuals may also have negative feelings toward biometrics because, historically, biometrics were linked to criminal investigations.

The counter arguments are that the benefits of biometrics far outweigh any concerns—especially in the midst of the COVID-19 pandemic. Biometric facial recognition is more accurate than the current human identity verification system, thereby enhancing safety and security. In addition, with respect to any alleged "bias" of biometrics technology, that technology is improving, and people are more likely to be "biased" than machines.

Further, there are state, federal, and international laws, as well as treaties and agreements, that govern the use of certain biometric data (such as passport and other identification photos for international travelers), and federal, state, and industry partners entering the biometrics arena have generally vowed to be conscious of and balance individual privacy with other goals. There are also existing U.S. databases that contain facial photos, so this technology would simply use those existing photos, plus the biometrics of anyone else who voluntarily chooses to participate in these biometric programs.

In addition, as set forth above, positive economic effects will result: primarily, the use of biometrics to create a safe, efficient, and healthy travel experience will reduce passengers' stress and increase satisfaction with the travel experience—no doubt to the benefit of airport shops, restaurants, and other retailers.

Conclusion

It remains to be seen if popular perceptions have evolved enough so that we will appreciate the convenience and security that biometric solutions can offer in the commercial aviation sector. Will travelers accept the use of biometric technologies because of the enhanced security, efficiency, and health benefits that they can provide? Only time will tell, but in the meantime, biometrics will continue to have an increasing effect on the air transportation industry.

Notes

* Elaine D. Solomon, a partner at Blank Rome LLP and co-chair of its aviation practice, is a member of the Board of Editors of *The Journal of Robotics, Artificial Intelligence & Law*. She concentrates her practice in the areas of aviation law and litigation, product liability, and tort litigation. Resident in the firm's office in Philadelphia, she may be contacted at solomon@blankrome.com.

1. *See Rosenbach v. Six Flags Entertainment Corp.*, __ N.E.3d ___, 2019, WL 323902 (Ill. Jan. 25. 2019).
2. PL 107-173.
3. PL 108-458.
4. PL 110-53.
5. *See* https://www.tsa.gov/biometrics-technology.