From Password to Person
The Evolution of Biometrics

May 2020

Table of contents

Executive Summary

In recent years, identity verifiers have moved to address the vulnerabilities of knowledge-based identity data by employing biometric solutions. The verification of biometric data, liveness detection, and associated security processing are key areas of innovation. Physical biometrics such as fingerprint, face, or palm are being combined with technologies that recognize behavioral traits and associated devices to create seamless, intelligent, and more secure methods of authentication.

This document:

- Provides a comparative overview of different biometric modalities
- Assesses security and usability issues
- Reviews recent advances in technology and the expansion of uses
- Discusses regulatory trends and ethical considerations

From Password to Person: The Evolution of Biometrics was produced in association with the International Center for Biometric Research and The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University.

Knowledge and Recognition

How can you be confident that someone is who they say they are?

Long ago, this wasn't a problem. Most people rarely interacted with anyone outside of their local village; they were recognized by sight, name, voice, or some other physical trait, and where necessary they were vouched for by a trusted third party. Over the years, methods evolved to aid identification, such as passports, ID cards, or driver's licenses—most of them anchored in the physical world. At the dawn of the digital age, a new question arose: How do you trust someone you don't know, can't see, and who isn't present in person? One solution has been the exchange of knowledge—passwords, PINs, memorable data, and personal details. But such techniques come at a price—loss of privacy, greater inconvenience, and rising rates of identity fraud. As a result, the password is being replaced by the person—be it thumbprint, facial imaging, voice inflection, or behavioral traits. As in the village of old, it's once again about recognition, but this time using techniques fit for a digital world.

SECURITY AND CONVENIENCE

For many years, there was a trade-off between security and convenience. More security meant less convenience—with ever more complex passwords, PIN numbers, memorable data, and CAPTCHA technology. Biometrics has changed that. More than 90% of users believe biometrics are more secure and more convenient than passwords and are willing to adopt biometrics to replace existing password-based authentication.[1]

Why Biometrics?

Think of the hundreds of accounts, passwords, PINs, and memorable (or forgettable) data you've accumulated. Most people forget a password at least once a month and attempt four passwords before they get it correct.[2] Or they jeopardize their security by re-using the same password across multiple devices and accounts. They choose passwords that are easy to remember and, for fraudsters, easy to guess. In the U.S. alone, there were 14.4 million victims of identity fraud in 2018.[3]

Biometrics offers a solution by enabling the automated recognition of individuals according to physical and, increasingly, behavioral traits. Physical traits can include the face, iris, and fingerprint, while behavioral traits might include the signature, keystroke, and habits of a phone or computer user.
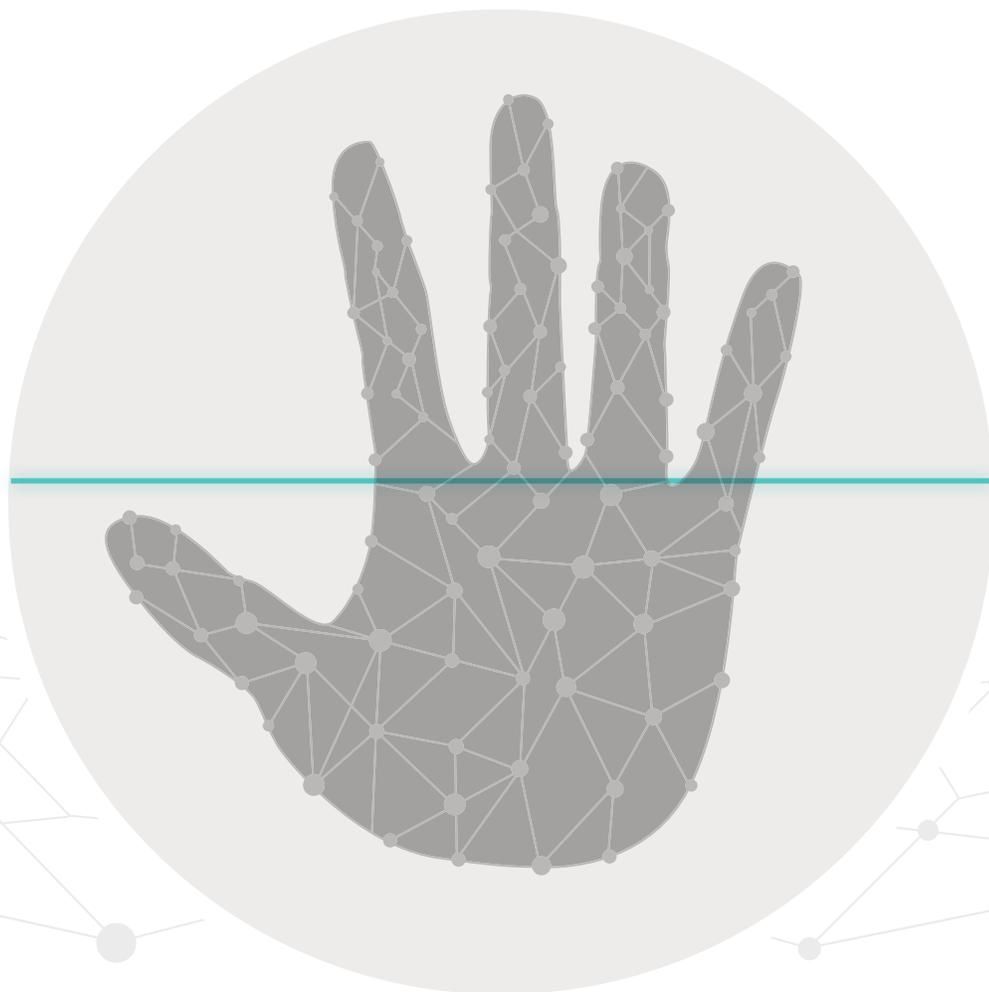
A Superior Experience

The alignment of superior user experience with superior security means that consumers increasingly use mobile biometrics for shopping and banking services. It is expected that by 2023, $2 trillion of transactions will be performed this way, up from $124 billion in 2018.[4]

Mobile Payment Security Forecast 2023[4]

37.2B
Biometric-authenticated transactions volume

$2T
Biometric-authenticated transactions value

80%
Proportion of smartphones with biometric hardware installed

1.5B
Number of smartphones using software-based facial recognition

57%
Proportion of biometric transactions that are remote transactions

51.6B
Number of contactless transactions that are tokenized

The Impact of the Smartphone

The arrival of biometrics on smartphones has been a key driver of innovation in this field. In 2011, Samsung released its first mobile device with face unlock[5] and, in 2013, Apple released its first fingerprint security feature on the iPhone 5S[6]. Since then, biometrics have revolutionized the mobile device market and have become a standard feature for security. By 2023, 80% of smartphones will have some biometric system attached to the phone.[7] Commercial apps that enable users to access account information over their smart devices can take advantage of the onboard, or native, biometric security capabilities. Some smartphones do not have native biometric security features. For these, biometrics like facial recognition, voice, and palm are still capable of operating without a dedicated sensor on the phone.

PRIVACY

A key security consideration is where and how biometric data used for authentication is stored. Some existing services collect consumer data in centralized databases and allow for identity attributes to be cross-matched with other information. Such centralized databases can be vulnerable to fraudsters. Each day, several million records are lost or stolen in data security breaches. Therefore, smartphones that are able to encrypt and store biometrics data on the phone itself offer a clear security advantage—an individual's identity is securely bound to a device that they own. Such considerations are increasingly relevant in an age when digital identity is becoming ever more important.[8]

Protecting Biometric Data

Hackers can steal passwords and PINs on an industrial scale, but the use of biometrics presents a bigger challenge to them. Where biometrics are native to the individual's device a large-scale breach is almost impossible—only that individual using that device can unlock the data. Non-native phone deployments are weaker, however—like PINs and passwords, the biometric data is stored elsewhere along with those of potentially thousands of others.

So the method of storing biometric data is key. Biometrics can be stored in three main ways: on servers, on the individual's device, or through visual cryptography. A drawback to using a centralized storage server is that it creates just one target for hackers to access hundreds of thousands of records. An example of a data breach on a server occurred in 2014 and 2015, when hackers breached the U.S. Office of Personnel Management (OPM) and stole approximately 21.5 million records of people's social security numbers, names, dates and places of birth, and addresses.[9] Also leaked in the data breach were roughly 5.6 million sets of fingerprints.[10]

On a user's device, the biometric template is stored in an encrypted format. Touch ID and Face ID data on iOS are stored in a security architecture called a Secure Enclave.[11] It cannot be accessed by the operating system (OS) or by apps—it is only used by the Secure Enclave to verify a user's biometrics to the enrolled template. Android devices use a Trusted Execution Environment (TEE)[12]. Similar to iOS, the TEE is separate from the phone's OS, making breaches of the device difficult. Another method for storing biometric data is visual cryptography[13], where the biometric template or image is split into two and stored at different locations. When a match needs to occur using the split template, the server can recombine the template to complete the authentication process.

In some cases, attacks are made at the sensor level, using spoofs to imitate a biometric sample in order to gain unauthorized access. Artificial fingerprints generated by machine learning methods have the potential to unlock around one-in-three fingerprint-protected smartphones.[14] The Samsung Galaxy S10's in-screen fingerprint sensor was also spoofed using a 3D printed fingerprint.[15] After the release of the Apple Face ID application in September 2017, Vietnamese cybersecurity firm Bkav used a 3D mask to spoof the depth mapping algorithm used in face recognition.[16] While noteworthy, such attacks have not been scalable.

Security, Convenience, and Thresholds

Biometrics need to be both secure and convenient to use. Determining the level of security and convenience is not an exact science. Consider an example: A customer of a financial institution uses biometrics to access their account. From a strict security standpoint, if a user places the correct finger on the sensor but positioned incorrectly, the system could make the user try again. However, how should the quality level be set such that the correct individual can gain access easily? There is an inherent trade-off between false accepts and false rejects. A false accept is when the incorrect person is accepted into the system; conversely, false rejects are rejecting users that should be allowed into their account. On a native system, this predetermined quality score is set by the operating system and the manufacturer, as opposed to an app in the third-party, non-native scenario.

Usability Factors

No matter how accurate biometrics are, they will only be effective if people trust them and want to use them. Traditional performance evaluations pay little attention to the usability of various modalities and how convenient people find them to interact with. If a system is troublesome, users will simply bypass the technology and jeopardize the adoption of biometrics in future applications.

Biometric systems should account for as much variation as possible in users since each sample acquisition will be different. To understand these variations, a biometric testing center was created at Purdue University. The International Center for Biometric Research (ICBR) has almost two decades of experience in testing biometric usability. Its research examines user habits, different biometrics (face, finger, iris, palm, ears, feet), environmental conditions (constrained, unconstrained, various lighting), and a variety of scenarios and devices. The ICBR leverages expertise in biometrics, ergonomics, and usability to investigate the interaction between human and biometric device, evaluate the impact of product design on system performance, and analyze user experiences. A brief overview follows.

Security, Convenience, and Thresholds

→ Fingerprint

Fingerprint sensors are affected by physiological features, placement of the sensor, and finger location.

Moisture, temperature, dirt, scars, and even worn-down fingerprints affect performance. Research analyzing the impact of age on image quality and performance has also shown differences, with the elderly adversely affected in particular.[17]

Figure 1: Examples of fingerprints from left to the right: high temperature, scarring, moisture, low definition, elderly.

The placement of the sensor on mobile or standalone devices is crucial to the performance of the biometric system—whether the front or reverse of the phone, in-screen or off-screen, the height of sensor, etc. Each of these positions has advantages and disadvantages that impact the user's ability to use the fingerprint sensor. Sensors on mobile devices are smaller compared to standalone fingerprint systems and can make it harder to place the correct portion of the finger on the sensor.

In testing at Purdue, certain fingers were observed to be easier than others for interacting with fingerprint systems. Subjects would often struggle using the ring and little fingers compared to the thumb, index, or middle finger.

Other research indicates higher failure to enroll (FTE) and failure to acquire (FTA) rates for smaller fingerprint images.[18]

Security, Convenience, and Thresholds

→ Face

Purdue has conducted facial recognition tests with occlusions such as hats and eyeglasses, variations of distance, different environments, and using different cameras.

Depending on how algorithms are trained to handle occlusions, subjects may still be verified; if the occlusions cover too much of the face, the subject is rejected due to a lack of features extracted. An example of a test subject's face that could extract facial features (left) and an image that failed to find a face (right) on commercial facial recognition software, is shown below in Figure 2. The positioning of the camera and lighting were the same—the only difference was the subject's hat.
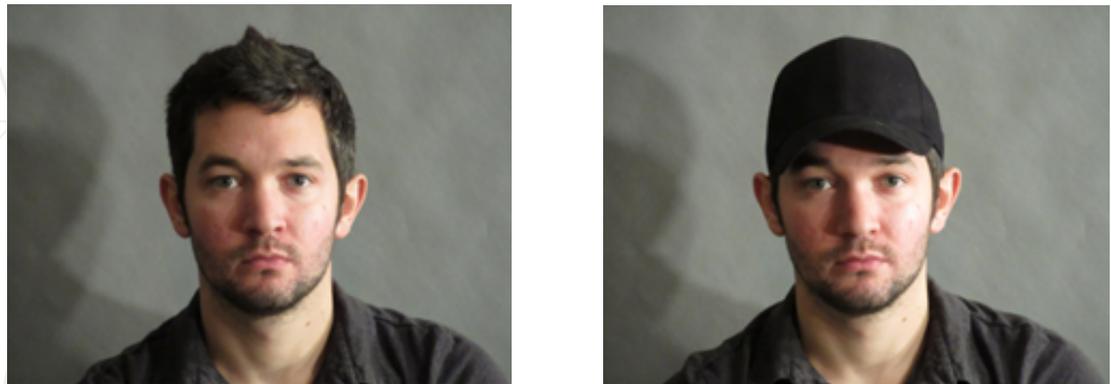

Figure 2: Extractable (left) and Unextractable (right) Facial Features

Another usability aspect of facial recognition is distance from the device. Subjects would often hold the camera further away if they were not satisfied with their appearance. Some applications fail to address this.

Environmental factors such as lighting affect the performance of the facial recognition system. Researchers at Purdue observed that bright sunlight changed the user's facial expression and created hot spots on the face, resulting in false rejects. Similar research also observed challenges of illumination and pose variation in uncontrolled environments[19].

Some cheaper devices still have difficulty acquiring successful samples in certain conditions (dark, light, occlusions) due to lower quality color sensors.

Security, Convenience, and Thresholds

→ Palm

Palm recognition is not as widespread as face and fingerprint but is gaining traction in healthcare environments because it is more hygienic. With a new technology that people do not understand, testing at Purdue has shown users struggled if they were not assisted through the entire sample acquisition process. In palm recognition pilots, users were briefed on how to use the applications but would often struggle to provide the correct location of palm, presenting the wrong side of the hand or placing it too close or far from the camera.

With phones becoming larger, some users have found it inconvenient to hold the phone with one hand while capturing the image with the other hand. This is also apparent in users with musculoskeletal disorders, like rheumatoid arthritis, who had trouble pressing a button and staying steady during acquisition.

→ Voice

The ICBR has observed difficulties with voice collection and analysis, although algorithms have improved to mitigate some of these challenges. Pronunciation of words by non-native speakers affects performance because of bias in voice recognition. Similar research confirms this.[20]

In mobile testing, the location of the speaker and the phone orientation affected sample acquisition. Android and iOS devices have different sensors in different places. When testing native Android users on iOS phones, for example, subjects didn't realize the speaker was located on the bottom of the phone. External noises also distract subjects, making it difficult to acquire samples.
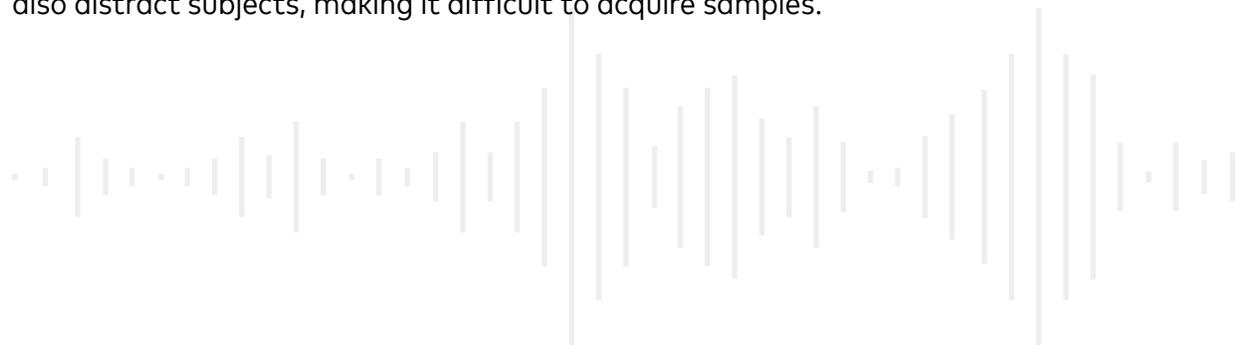
Passive Biometrics
and Behavioral Analytics

Physical (a.k.a. 'explicit') biometrics compare physiological credentials to a verified match. However, in the real world, we rely on more than just physical appearance to identify an individual.

Consider a hypothetical example: Ella has a pet cat, Lyra. One way Ella recognizes Lyra is by appearance; the animal's color and physical dimensions (explicit). Ella's confidence in her recognition increases if Lyra is in Ella's home at the moment of verification, because that is where she expects to find the cat (context); confidence rises even further when the cat chooses Lyra's favorite cushion to sit on and responds to her name (familiar behavior).

Take another example: Ella's neighbor Lyn drops by to borrow her lawnmower. Ella feels confident about lending the mower because she recognizes Lyn (physiology, context), Lyn has borrowed it before (history), and Ella assesses the risk of losing the lawnmower as low (intelligence). All of these factors play a part in building a level of confidence in a particular interaction.

In much the same way that Ella recognizes Lyra and Lyn, advanced machines using AI are capable of learning to recognize only those aspects of an individual's behavior that are relevant to the task at hand. These techniques are increasingly being used in authentication to identify bad actors trying to masquerade as legitimate users. In mobile commerce, for example, behavioral analytics can assess the passive biometrics of how an individual interacts with their phone: how they type, swipe, and navigate websites and apps. From those individual data points, a valid user profile can be created that is difficult for fraudsters to spoof.

Crucially, authentication techniques that apply intelligence to passive biometrics don't require extensive knowledge of the individual. They only need to recognize the individual and the situation at hand. Ella doesn't need to know Lyn's date or place of birth, her criminal record, her bank balance, or maiden name in order to lend her the lawnmower. She only needs to know enough to recognize Lyn and to be confident that she can be trusted with her lawnmower.

Passive Biometrics and Behavioral Analytics

This distinction between knowledge and recognition is very important in an era when privacy and data ethics are under increased scrutiny. There is growing resistance to crude identity verification techniques reliant on the repeated disclosure of static personal information, passwords, and PINs.

By applying advanced analytics capabilities to passive biometrics, establishing identity becomes a dynamic, real-time, and more accurate process—continuous verification. Continuous verification combines multiple behavioral biometrics that work passively as a user interacts with their device. Just as every fingerprint, face, or iris may be different, the way in which a person uses a particular finger to type, swipe, or text is unique too. The goal of continuous verification is to create a secure solution that verifies the individual without them being aware of an additional layer of explicit security. In the field of payments, for example, Mastercard applies AI to hundreds of data points both before and during a given transaction in order to accurately identify and help mitigate risk.

CONTINUOUS VERIFICATION

Passive biometrics, behavioral analytics, and advanced risk assessment are dramatically enhancing identity verification in the digital realm. The process of authentication begins when a consumer arrives at a merchant site, detecting anomalies in behavior and environment that may indicate bad actors. Risk-based authentication uses advanced intelligence to generate a risk score that is continuously updated throughout the process.

Recent Advances in Biometrics

Technology

→ Touchless Fingerprint Scanners

IDEMIA, FlashScan, and Touchless Biometric Solutions (TBS) have developed fingerprint sensors that can acquire fingerprint images by using advanced 3D imaging technology, which requires no interaction with/touching of the device. The touchless technology manages wet and dry fingers, eliminates ghost images left on the scanner, and addresses hygiene concerns.

→ In-Display Fingerprint Readers

Fingerprint scanners that use very high-frequency sound are being deployed in the newest models of Android phones, such as Samsung's Galaxy S10. The sound maps the 3D contours of a finger through the glass in order to identify the owner and unlock the device.

→ Fingerprint on Card

In 2017, Mastercard launched its first biometric card, combining fingerprints with chip technology for a more secure transaction.[21] The card features an embedded fingerprint sensor to quickly capture and match the cardholder's fingerprint to the digital fingerprint image stored on the card.

→ 3D Facial Recognition

Companies such as Apple, KeyLemon, and IDEMIA have developed 3D facial recognition technology to measure the geometry of rigid features of the face. 3D facial recognition can even be used in dark environments and can recognize a person at different angles of up to 90 degrees. The advanced camera technology captures facial data by projecting and analyzing thousands of points on a depth map, while also capturing an infrared image of the face.

→ Long-Range Iris Recognition

Researchers from Carnegie Mellon University were able to use iris recognition technology to identify drivers from an image of their eye captured from up to 40 feet (12 meters) away.[22] In addition to improving security, passive technology is more convenient for individuals.

Recent Advances in Biometrics

➔ Spoof and Liveness Detection Software

Biometrics can be spoofed to gain unauthorized access to someone's information. Researchers have further developed spoof and liveness detection software to recognize fake biometric samples. Depending on the modality, liveness detection is accomplished by prompting users to act (blink or rotate head for face recognition) or is performed by algorithms that detect indicators of non-living images.

➔ Machine Learning and Artificial Intelligence

Traditionally, biometric algorithms have been pattern recognition systems, but new techniques such as machine learning and artificial intelligence are becoming more popular. Facebook's face recognition system, DeepFace, and Amazon's, called Rekognition, both use machine learning. The performance of traditional biometric systems can be hampered by poor quality or partial biometric samples, but ML and AI algorithms deal with poor-quality images more effectively. Their performance improves as the number of samples increases. As more data is given to the system, the smarter it becomes in recognizing it.

Expansion of Uses

➔ Internet of Things

The physical and digital worlds are merging. In an era of hyper-connectivity, people are never really offline. By 2022, there will be an estimated 50 billion connected devices and sensors on the planet.[23] They manage access to connected homes, buildings, and cars, operate appliances, and control industrial processes. Such devices need to be identified and their actions authenticated without the creation and use of further accounts and passwords by the individual. Biometric solutions enable the secure management of devices without adding friction to the process.

➔ Travel

Travel is a sector where biometric technologies are developing fast. In part, this is because of the multiplicity of checkpoints and high levels of security required. By 2037, it is estimated that 8.2 billion people will pass through airports.[24] Facial recognition, fingerprint, and iris scanning are all deployed currently. British Airways claims that facial recognition technology at departure gates allows it to board 400 passengers in just 22 minutes.[25] In 2021, European Union member states will be asked to collect facial data and fingerprints from all third-country nationals entering the EU. CLEAR, a biometric security company commonly employed at airports, is expanding into retail and healthcare.[26]

Recent Advances in Biometrics

→ Workplace

Biometrics are increasingly used by employees to enter their place of work, log in to phones and computers, and access data storage areas. A recent survey suggested that nearly two-thirds of IT companies have adopted biometrics for security, employee access, and/or data security management. An additional 24 percent said they plan to implement biometrics by 2020.[27]

One biometric software that is being utilized for access control in the workplace is Microsoft's Windows Hello. Windows Hello allows employees to use face or fingerprint recognition rather than a PIN or password to gain access to their device. The director of program management in Microsoft's identity division, Alex Simons, said, "Passwords are the weak link. They have terrible characteristics about them, and they're hard for you to keep track of. Passwords are also super expensive for companies."[28] He revealed that Microsoft alone spent over $2 million each month on help desk calls from customers seeking assistance to change their passwords.

Continuous authentication is another biometric solution companies are using to keep data and employees secure. As previously discussed, continuous authentication learns behavioral patterns and can identify when unauthorized individuals are trying to access information. The software runs in the background on a personal computer or handheld device and learns how someone holds the phone, their typing mannerisms, and how they scroll or toggle between screens.

→ Healthcare

Patient safety and privacy have long been important issues for healthcare providers. In a single year, thousands of patients in the UK received the wrong treatment because of identification errors.[29] To combat such issues, healthcare providers and hospitals are increasingly employing biometric security solutions such as palm-vein scanning[30] for patients and fingerprinting newborn babies and their mothers.[31]

Automated Medication Dispensing Cabinets (ADC) with fingerprint recognition are being adopted to help regulate medication and prevent potentially harmful errors and adverse drug events. The market for ADC technologies is expected to expand from $3.57 billion in 2018 to $6.21 billion by 2026.[32]

Ethical Considerations and Policy

Privacy and ethical issues have arisen since the deployment of automated biometric technologies. Bias issues, for example, have hampered the widespread adoption of the technology in its current state. Various studies have noted that biometric algorithms can struggle to recognize some races, ethnicities, darker skin pigmentations, and genders. Researchers at MIT found that the leading face recognition algorithms (Microsoft, Face++, and IBM), produced less accurate results for darker males and females compared to individuals with lighter skin.[33] As such, the technology has been restricted around the U.S.[33,35,36,37] and has raised concerns in Europe.[38,39] In the field of social media, Facebook attracted criticism following reports that users' photos were used to train Facebook's face recognition algorithm DeepFace without their knowledge.[40]

Biometric standards committees have evolved to facilitate interoperability, data exchange, and consistency of use. Similarly, best practices have been developed to inform the deployment of biometrics, such as Oxford University's Five Factor Framework[41] for financial services (i.e., modality performance, usability, interoperability, security, and privacy).

Biometric methods are preferred by regulators and standard-setters who advocate strong customer authentication. However, data and privacy concerns have prompted the creation of new legislative frameworks. The European Union's General Data Protection Regulation (GDPR) protects EU citizens and residents from the sharing of their biometric data with third parties, makes clear and affirmative consent a requirement, and establishes the right to be forgotten. In the U.S., a patchwork of mandates has evolved at federal and state levels to regulate the use of biometric data. In Florida, lawmakers banned the use of biometrics in their education system in order to protect student's biometric data.[42] Illinois passed a law requiring companies to let users know when biometric data are collected and how the data will be used. Washington and Texas have since passed similar laws.[43] In California, home to Silicon Valley, the California Consumer Privacy Act established a framework similar to the GDPR.

However, the evolution, and improvement, of biometrics authentication is encouraging its adoption. A recent research suggests that more than 90 percent of users "believe biometrics are more secure and convenient than passwords". [44] For the adoption of these technologies to be successful, transparency and engagement need to be at the forefront for integrators.

Conclusion

Effective biometrics melt into the broader experience of consumer-centric services, giving people the power to transact with minimal exchange of personal data. The advent of biometric solutions has prompted a shift from knowledge-based methods of verification to those that employ intelligent recognition—replacing the password with the person. The continued adoption of such technology is dependent on users' faith in its safety and effectiveness. As biometrics expands to new use cases in healthcare, travel, and the workplace, we strongly recommend that practitioners advance trust through security-by-design, an approach to biometric innovation that places the protection of data and identity at the heart of the technology.

1. Mobile Biometrics in Financial Services: A Five Factor Framework, University of Oxford, Mastercard, https://newsroom.mastercard.com/eu/files/2017/06/Mobile-Biometrics-in-Financial-Services_A-Five-Factor-Framework-compressed3.pdf

2. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services, Virginia Tech, 2018, https://people.cs.vt.edu/gangwang/pass.pdf

3. 2019 Identity Fraud Study, Javelin Strategy & Research, https://www.globenewswire.com/news-release/2019/03/06/1748662/0/en/Consumers-Increasingly-Shoulder-Burden-of-Sophisticated-Fraud-Schemes-According-to-2019-Javelin-Strategy-Research-Study.html

4. 5 ways biometrics are going mainstream for payments, PaymentsSource, https://www.paymentssource.com/list/5-ways-biometrics-are-going-mainstream-for-payments

5. Face Unlock - Android 4.0 Ice Cream Sandwich 4.0's Most Personal Feature - Android Authority. (2011), https://www.androidauthority.com/face-unlock-android-4-0-ice-cream-sandwich-most-personal-feature-27693/

6. iPhone 5s-Technical Specifications, from https://support.apple.com/kb/sp685?locale=en_US

7. 5 ways biometrics are going mainstream for payments, PaymentsSource, https://www.paymentssource.com/list/5-ways-biometrics-are-going-mainstream-for-payments

8. Restoring Trust in a Digital World, Mastercard, 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf

9. Massive Data Breach Puts 4 Million Federal Employees' Records At Risk: The Two-Way – NPR, https://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk?t=1573213084279

10. OPM Announces 5.6 Million People's Fingerprints Were Exposed in Data Breach - The Atlantic, https://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/

11. About Touch ID advanced security technology - Apple Support, https://support.apple.com/en-gb/HT204587

12. How does Android save your fingerprints? - Android Central, https://www.androidcentral.com/how-does-android-save-your-fingerprints

13. Ross, A., & Othman, A. (2011). Visual cryptography for biometric privacy. IEEE Transactions on Information Forensics and Security, 6(1), 70–81. doi:10.1109/TIFS.2010.2097252

14. Bontrager, P., Roy, A., Togelius, J., Memom, N., & Ross, A. (2018). DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. IEEE International Conference on Biometrics: Theory, Applications and Systems.

15. Samsung's Galaxy S10 fingerprint sensor fooled by 3D printed fingerprint - The Verge (2017), https://www.theverge.com/2019/4/7/18299366/samsung-galaxy-s10-fingerprint-sensor-fooled-3d-printed-fingerprint

16. This $150 mask beat Face ID on the iPhone X - The Verge (2017), https://www.theverge.com/2017/11/13/16642690/bkav-iphone-x-faceid-mask

17. S. K. Modi, S. J. Elliott, J. Whetsone and H. Kim, "Impact of Age Groups on Fingerprint Recognition Performance," 2007 IEEE Workshop on Automatic Identification Advanced Technologies, Alghero, 2007, pp. 19-23. doi: 10.1109/AUTOID.2007.380586

18. Liu-Jimenez, J., Ros-Gomez, R., Sanchez-Reillo, R., & Fernandez-Saavedra, B. (2016). Small fingerprint scanners used in mobile devices: the impact on biometric performance. IET Biometrics, 5(1), 28–36. doi:10.1049/iet-bmt.2015.001

19. Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. ACM computing surveys (CSUR), 35(4), 399-458

20. Voice Recognition Still Has Significant Race and Gender Biase, Harvard Business Review, https://hbr.org/2019/05/%20voice-recognition-still-has-significant-race-and-gender-biases

21. Biometric EMV Card by Mastercard | EMV Card with Fingerprint Reader, https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html

22. Venugopalan, S., Prasad, U., Harun, K., Neblett, K., Toomey, D., Heyman, J., & Savvides, M. (2011). Long range iris acquisition system for stationary and mobile subjects. In 2011 International Joint Conference on Biometrics (IJCB) (pp. 1–8). IEEE. doi:10.1109/IJCB.2011.6117484

23. The Internet of Things: Consumer, Industrial & Public Services 2018-2023, Juniper Research 2018

24. IATA Forecast Predicts 8.2 billion Air Travelers in 2037, IATA, https://www.iata.org/pressroom/pr/Pages/2018-10-24-02.aspx

25. How Biometrics is Reshaping the Travel Experience, ttg, https://www.ttgmedia.com/news/technology/how-biometrics-is-reshaping-the-travel-experience-17642

26. San Francisco Facial Recognition Ban May Give You Wrong Impression, CNBC, https://www.cnbc.com/2019/05/15/san-francisco-facial-recognition-ban-may-give-you-wrong-impression.html

27. More Employers Are Using Biometric Authentication, SHRM, https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employers-using-biometric-authentication.aspx

28. Beyond passwords: Companies use fingerprints and digital behavior to ID employees, CNN, https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html

29. 24,000 patients get wrong treatment, Metro News, https://metro.co.uk/2007/07/11/24-000-patients-get-wrong-treatment-510891/

30. Harris Health System has 500+ Maria Garcias—with the same birthday. Here's how it keeps them straight, Advisory Board Daily Briefing, https://www.advisory.com/daily-briefing/2019/02/20/biometrics

31. Researchers Develop Biometric Tool for Newborn Fingerprinting, UC San Diego Health, https://health.ucsd.edu/news/releases/Pages/2018-09-12-researchers-develop-biometric-tool-for-newborn-fingerprinting.aspx

32. Automated Dispensing Machines Market To Reach USD 6.21 Billion By 2026, Reports And Data, https://www.globenewswire.com/news-release/2019/08/08/1899365/0/en/Automated-Dispensing-Machines-Market-To-Reach-USD-6-21-Billion-By-2026-Reports-And-Data.html

33. Raji, I. D., & Buolamwini, J. (2019). Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products. Artificial Intelligence, Ethics, and Society.

34. Oakland bans use of facial recognition technology, citing bias concerns, San Francisco Chronicle, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

35. San Francisco Bans Facial Recognition Technology, The New York Times, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

36. Somerville City Council passes facial recognition ban, The Boston Globe, https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html

37. State Bill Would Ban Facial Recognition and Biometric Technologies from Police Body Cameras - KQED News, https://www.kqed.org/news/11753753/state-bill-would-ban-facial-recognition-%20and-biometric-technologies-from-police-body-cameras

38. Inside the urgent battle to stop UK police using facial recognition, Wired, https://www.wired.co.uk/article/uk-police-facial-recognition

39. Europeans still anxious about AI facial recognition – EURACTIV.com. https://www.euractiv.com/section/data-protection/news/europeans-still-anxious-about-ai-facial-recognition/

40. What to Do If You're Missing Facebook's Face Recognition Setting - Consumer Reports, https://www.consumerreports.org/privacy/what-to-do-if-youre-missing-facebooks-face-recognition-setting/

41. Mobile Biometrics in Financial Services: A Five Factor Framework, University of Oxford, Mastercard, https://newsroom.mastercard.com/eu/files/2017/06/Mobile-Biometrics-in-Financial-Services_A-Five-Factor-Framework-compressed3.pdf

42. Florida Bans Use of Biometric Data in Schools | The National Law Review. https://www.natlawreview.com/article/florida-bans-use-biometric-data-schools

43. Businesses and courts continue to struggle with Illinois biometric privacy law scope, Biometric Update.Com, https://www.biometricupdate.com/201910/businesses-and-courts-continue-to-struggle-with-illinois-biometric-privacy-law-scope

44. Mobile Biometrics in Financial Services: A Five Factor Framework, University of Oxford, Mastercard, https://newsroom.mastercard.com/eu/files/2017/06/Mobile-Biometrics-in-Financial-Services_A-Five-Factor-Framework-compressed3.pdf