# *Authentication Using Biometrics: How to Prove Who You Are*

**Robert Hummel, PhD; Timothy W. Bumpus, PhD; Alyssa Adcock, PhD; and Sharon Layani**

*STEPS: SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES*

*STEPS* Issue 5 (2021): 25-35.

STEPS (Print) ISSN 2333-3219
STEPS (Online) ISSN 2333-3200

STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

ISSUE 5, 2021

Robert Hummel, PhD
*Editor-in-Chief*

IN THIS ISSUE

Articles

POTOMAC INSTITUTE PRESS

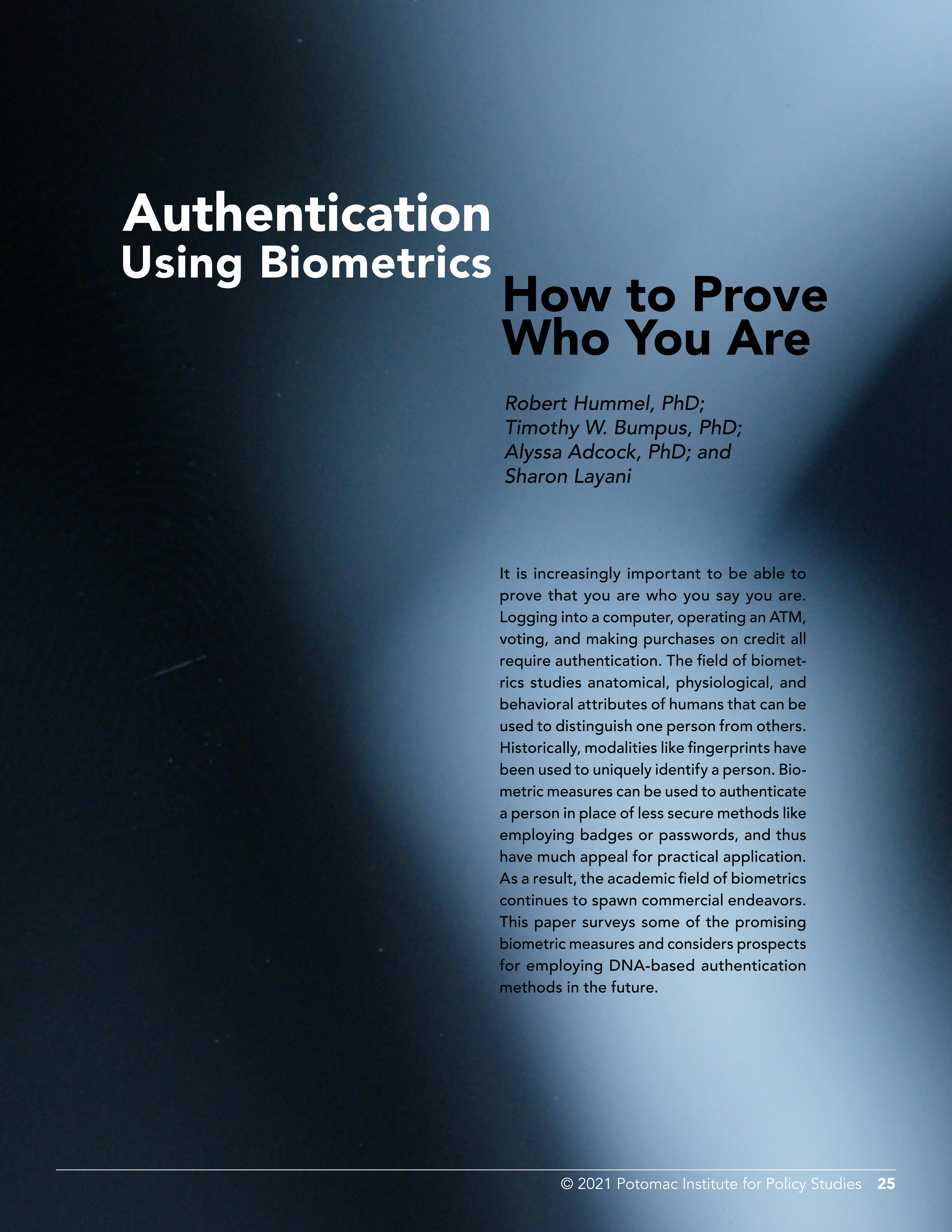
**Cite this article:** Robert Hummel, Timothy W. Bumpus, Alyssa Adcock, and Sharon Layani, "Authentication Using Biometrics: How to Prove Who You Are" *STEPS* 5 (2021): 25-35. Available from: https://www.potomacinstitute.org/steps/featured-articles/98-authentication-using-biometrics-how-to-prove-who-you-are.

POTOMAC INSTITUTE PRESS

*STEPS: Science, Technology, Engineering, and Policy Studies*
is published by Potomac Institute Press of the
Potomac Institute for Policy Studies.

**Disclaimers:** The Publisher, Institute, and Editors cannot be held responsible for errors or any consequences arising from the use of information contained in this publication; the views and opinions expressed do not necessarily reflect those of the Publisher, Institute, and Editors. The Potomac Institute is non-partisan and does not take part in partisan political agendas.

Access to *STEPS* is available free online at:
www.potomacinstitute.org/steps.



# Authentication Using Biometrics

## How to Prove Who You Are

*Robert Hummel, PhD;*
*Timothy W. Bumpus, PhD;*
*Alyssa Adcock, PhD; and*
*Sharon Layani*

It is increasingly important to be able to prove that you are who you say you are. Logging into a computer, operating an ATM, voting, and making purchases on credit all require authentication. The field of biometrics studies anatomical, physiological, and behavioral attributes of humans that can be used to distinguish one person from others. Historically, modalities like fingerprints have been used to uniquely identify a person. Biometric measures can be used to authenticate a person in place of less secure methods like employing badges or passwords, and thus have much appeal for practical application. As a result, the academic field of biometrics continues to spawn commercial endeavors. This paper surveys some of the promising biometric measures and considers prospects for employing DNA-based authentication methods in the future.

## Introduction

It is hard to prove that you are who you say you are.

You have a name, and so you can tell people your name. But someone else could impersonate you by using the same name. What do you do if you have to prove that you are the person that you say you are?

Of course, we must prove it all the time. We sign documents, we provide passwords to log in, and we present photo IDs. Sometimes we are required to provide our social security number and date of birth, as though only we would know that information. Notaries check our government-issued picture IDs, as do the TSA officials at the airport. Increasingly, voting locales require some form of identification. Physical possession of a smartphone also acts as a personal identifier. Now, we can make purchases based on possession of our personal cell phone.

None of these methods of authentication are fool proof. For example, signatures morph over time and are forgeable. Databases of identification numbers are stolen. Passwords are hacked. Cell phones are stolen and unlocked. A determined impersonator can defeat any of these authentication approaches.

Identity fraud and identity theft are increasingly serious problems costing tens of billions of dollars per year in the US alone. All interactions with government, with financial institutions, and most interactions with businesses involve authentication as proof of identity. It is fundamental to our workings as a civilized society. The election security debate is mostly about trust in authentication. Technology, however, can provide solutions.

An unacceptable solution is to install a chip into every human upon birth. In lieu of this distasteful solution, society is increasingly turning to technology and employing biometrics to authenticate a person. Biometrics are unique physiological and behavioral attributes that can be used to identify individuals. These characteristics are individualized, relatively fixed, and recordable. Typically, they are also hard to forge. In what follows, we discuss the emerging possibilities for automated biometric authentication.

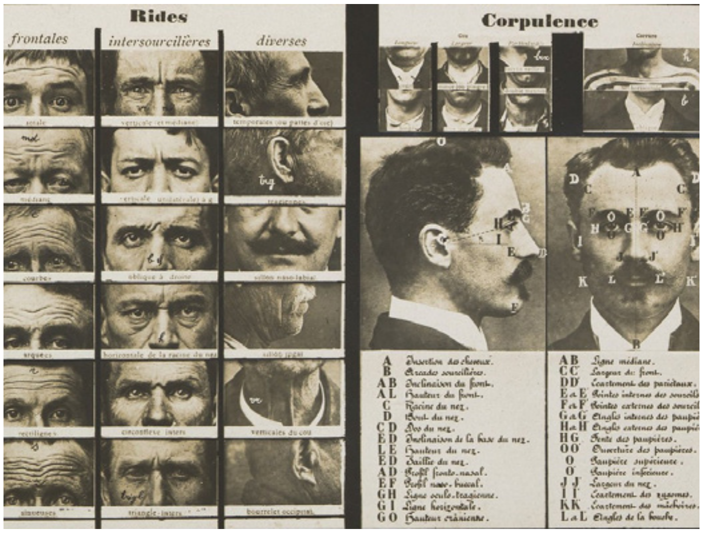
Ultimately, the most unique and immutable property of each individual is their DNA sequence. (Of course, identical twins have the same DNA sequence, but there are other markers to distinguish them.) By identifying an appropriate number of specific markers that vary across the population, but uniquely identify a particular individual, it should be possible to biochemically authenticate a person. With advances in biotechnology, we foresee a time when signatures can be replaced with fast and efficient biochemical tests.

Authentication of an individual is only one aspect of a broader set of applications of identity management. Biometrics can be used to identify a single person in a crowd or to label each person presented to a system. Authentication refers to a specific case, where a person is either an impersonator or not. Impersonation will be uncommon, but for many applications it is important that impersonators are deterred or caught.

## The Biometric Database

The concept of using biometric data for authentication is to demonstrate that a set of traits unique to a person match a prior recorded registration of those traits. The pre-stored database associates identity with the biometric data. The recorded data can be stored locally to the individual in an unalterable form or can be accessed remotely. Information technology allows us to access such a database quickly, and the fact that the individual claims an identity means that accessing the appropriate record is easy and does not require a search (although a search is also generally easy).

The stored database needs to be secure, or else an imposter can change the associations. Moreover, stored biometric data will often be classified as personally identifiable information, protected health information, or individually identifiable health information. These categories of information are covered by regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and various state regulations, and so must be kept protected. While compromised passwords can be changed, compromised biometric information is not easily changed. Public key encryption and homomorphic access technologies to compare sampled data with the encrypted stored data are possible solutions to maintain security. However, compromises from hacking are always possible, and privacy concerns exist across much of civil society with respect to biometric technologies.



Alphonse Bertillon's Synoptic Table of Physiognomic Traits (ca. 1909).

## Types of Biometrics for Authentication

Detailed ways of identifying people based on unique traits dates to the Bertillon System of 1879. Bertillon's system collected measurements to accompany a photograph of the subject and recorded the data on a filing card to track individuals in the criminal justice system. Bertillon's system captured five main measurements—the head length, head breadth, the length of the middle finger, the length of the left foot, and the length of the cubit (the length of the forearm).[1] While these measurements were not exactly unique and did lead to a few mistaken identity events,[2] they represent an early approach to systematic identity management. Today's "mugshot" is a direct hold-over from this approach.

More modern types of biometrics range across multiple modalities and can be categorized as external physiology, behavioral, and internal physiological. Table 1 lists examples of biomarkers that can be used as biometrics, within categories. Most can be used to help authenticate a person, to provide entry, or to permit authorized actions. Some biometrics provide binary data: they either match or they don't. Other biometrics are analog, and match only if the value is close enough. When used for authentication and referencing encrypted stored values, the associated encryption method needs to preserve "nearness" for such analog measures. For search, filtering, and identification applications, machine learning approaches might be useful in training the recognition system. For authentication, however, machine learning will be useful for finding features in the data that might be best extracted to do the comparison for verification, and a separate decision procedure is needed to decide if the features match the pre-stored features for each authentication instance.

In the next section, we provide more details for current and future biometrics that can be used for authentication, and in many cases other forms of identification.

## Current and Future Directions

Certain biometrics for identity authentication have been around for ages and are mature technologies, while others are emerging and still under development. There is often little data about performance levels because the accuracy depends so heavily on the particular application, operating environment, and the distribution of the population being presented. The following is a survey of selected biometric modalities.

### *Face Recognition Systems*

Humans use face recognition as the primary method of identifying people that they meet. Automated face recognition using image processing traces its roots to 1964 and the work of Bledsoe et al., who proposed identification based on 21 measurements.[3] Since then, face recognition has been a mainstay of computer vision research. Recognition often compares facial features based on the spacing of the eyes, the bridge of the nose, the contour of the lips, ears, and chin. Other approaches use features such as the residuals after a principal components decomposition of a cropped image of the face.[4] More recent developments include the use of machine learning for automated feature extraction and recognition against a database of stored faces.[5,6]

Commercial and government applications of face recognition are now standard. Some retail stores use facial recognition to identify returning shoppers.[7] Governments use facial recognition for border control. Non-cooperative access control for computers or physical portals can make use of face recognition. Authentication for logins to web accounts, such as Microsoft, Amazon, Google, and Facebook are valuable enhancements and explains why these companies have interest in face recognition. Other companies and agencies can monitor access to facilities using face recognition to supplement badge readers. Reports of widespread use of

Table 1. Examples of biomarkers that can be used as biometrics, within categories.

| Category | Biometric | Description |
|---|---|---|
| External physiological | Voice | Identification based upon personal voice tracts |
| | Facial recognition | Identification by matching features from a map of facial features |
| | Fingerprints | Pattern recognition of the unique features of a fingerprint |
| | Palm prints | Similar to fingerprints, but not as widely used |
| | Hand geometry | Identification through the shape and dimensions of the hand |
| | Iris | Measuring the iris texture through visible and near-IR light to create a unique profile |
| | Ear shape | Similar to facial recognition but uses a detailed profile of the ear |
| | Scars | Considered a "soft" biometric identified along with marks and tattoos to identify an individual |
| | Eye veins | Using pattern-recognition on video images of the veins of the eyes |
| | Periocular | "Eye" recognition that includes the eyelids, eyelashes, eyebrows, tear duct, eye shape, and skin texture |
| | Odor | Characterizing and recognizing an individual based on their odor |
| | Footprint | Measuring the geometry, shape, and texture of footprints for identification |
| | Skin reflection | Using spectral reflectance of the skin for identification |
| Internal physiological | Sweat | Analyzing a profile based on amino acids and other compounds of each user from a sweat sample |
| | Blood and urine | Analysis of blood and/or urine samples. Blood samples can also be used to get DNA samples |
| | Microbiome | Using microbe data from stool, saliva, skin, and other collection sites, it has been shown that identification is possible and some samples remained stable for >80% of study participants after 1 year |
| | EEG/ECG | Taking EEG, ECG, or similar signals collected during a perception or mental task for identification purposes |
| | Tissue | Can include 2D ultrasound biometric systems. Direct tissue samples can also be used to get DNA samples |
| | Saliva | Saliva samples can be used to extract DNA samples |
| Behavioral | Typing habits | Based on monitoring how a user types, identity and mood can be identified |
| | Signature | Includes writing rhythm, acceleration, and habits |
| | Gestures | Generally captured from the face or hand; can classify and identify human motion |
| | Gait | Monitoring and modeling the way someone walks to identify them |
| | Touch screen tendencies | Integrating authentication into interaction based on personal tendencies on how a user touches a screen to ensure security |
| | Accelerometer data | A behavioral biometric identifier built around a user's movements |
| | How a device is held | Similar to touch screen tendencies and the accelerometer data, how a device is held can also build up a behavioral data set |

facial recognition in China suggest population control. As a result of these and many other applications, there are many companies vying as suppliers of facial recognition technology.[8] Further, these technologies are available worldwide. Some face-searching tools are accessible to anyone as companies are able to capitalize on images others upload to the internet.[9]

Face recognition technology is controversial. Some contentious issues include government use of face recognition to track individuals, perform suspect law enforcement activities, repress disfavored ethnic groups, and generally violate privacy rights. Moreover, the technology has been shown to exhibit higher false positive rates for people of darker skin color,[10] and potentially other ethnic biases. As a result, legal restrictions have been placed on the use of face recognition in certain jurisdictions.

Due to years of research progress, face recognition works quite well when evaluated in laboratory settings. Typical benchmark reports show better than 99% accuracy,[11] others with error rate of less than 1%,[12] depending on the number of faces in the pallet of possibilities. Algorithmicists compete internationally: The GaussianFace algorithm developed in 2014 at The Chinese University of Hong Kong achieved facial identification scores of better than 98%.[13] In 2020, one facial recognition algorithm test had an error rate of 0.08%.[14]

For face recognition of images and video "in the wild," performance figures are less readily available. Performance must be measured in the context of the application and can vary with collection geometry and lighting. As an example, Apple claims that there is a 1-in-1,000,000 chance that a random person can unlock an iPhone using FaceID®,[15] but false rejection is less important because one can simply use a passcode in lieu of the biometric. Further, false rejections might not be evenly distributed across the population. Certain faces might be harder to authenticate, because they are too nondescript.

### *Fingerprinting*

Fingerprint recognition is one of the oldest and most developed biometric recognition methods. Latent fingerprint identification has been used forensically since at least the 19th century.[16] Today, automated fingerprint recognition for authentication is regularly used for access control. The FBI maintains the Fingerprint Identification Records System and uses the Integrated Automated Fingerprint Identification System (IAFIS) to match fingerprints against the database. Fingerprint-based access control systems for computer access or physical portal control are available commercially.[17] Many laptops now have built-in fingerprint readers to control login access and use of a password manager, although the software generally allows for a password-based backup in case the fingerprint identification falsely rejects the user. As another example, the airport screening company Clear uses biometrics to authenticate people, with fingerprints as one of the biometrics that can be used.

Historically, fingerprints were collected using ink impressions on cardboard cards. Now, fingerprints can be collected using optical approaches, and can even be obtained by contactless methods. Contact systems can use an image, or measure conduction from a capacitive surface. Certain smartphones now use ultrasonic sensors to collect fingerprints. Contactless fingerprint technologies include commercially available contactless fingerprint scanning technologies, with at least four mobile (smartphone-based) apps and two stand-alone contactless devices on the market.[18] Contactless devices generally require that the fingers are in close proximity to the reader, but a fingerprint of a German defense minister was famously digitally recreated from photos.[19]

The technology for recognizing fingerprints can use a direct comparison of the stored image of the fingerprint against the scanned print, invariant to a certain amount of variation of position and angle. However, this approach can fail to align the features accurately, and so the established method of recognizing fingerprints is by observing specific features (such as loops, whirls, and arches), categorized manually, or extracted automatically using image processing. Biometric identification research continues to include developing improvements to fingerprint recognition, especially for contactless technologies.[20]

The accuracy of fingerprint identification is highly variable, and controversial.[21] For authentication, most systems will establish a loose threshold, with the assumption that imposters will be rare. Crime-solving using fingerprints is well established, but often makes use of other evidence to help narrow the search and improve the apparent accuracy of the fingerprint identification.

### *Automated Signature Verification*

The earliest surviving signature is from 3100 B.C.E.,[22] signifying the importance of signatures for authentication. Automated signature recognition can either be static, i.e., comparing one total signature image to another, or dynamic and can involve additional data such as the coordinates, pressure, azimuth, and inclination. Automated signature recognition has been a continuing research application of image processing, both historically,[23] and more recently.[24] Signature verification is heavily used in banking, real-estate, and government applications. Numerous software vendors supply software systems to support signature identification.[25,26]

There are currently many studies looking at the accuracy of signature recognition. However, scores need to be interpreted in the context of whether one is attempting to reject random forgeries or skilled forgeries.[27] For true positives, there is the issue that signatures naturally change over time and thus require certain tolerances to be accepted. There are famous examples of forgeries that have evaded detection by experts (at least initially) such as the Hitler Diaries.[28] Often celebrities' signatures sold online have been found to be faked. Research goals would hope to make automated signature verification as good as expert manual verification, but current systems are likely not that good.

### *Hand Geometry and Palm Prints*

In addition to fingerprint recognition, hand geometry (the use of hand measurements) as a biometric has received much research interest.[29,30] Hand geometry can be combined with palm prints for higher accuracy, using such measures as the area of the hand, and the length/width of fingers, and palm print features such as lines, wrinkles, minutiae, and delta points.[31] Using IR sensors, one can combine information from the structure of veins in the hands and fingers.[32,33] The goal is to develop a contactless verification system wherein one could wave a hand that would then be evidence of one's identity.[34,35]

While much of the hand and palm recognition development is in academic research, since 2013 the FBI has maintained the National Palm Print System of millions of palm prints. Many anticipate rapid growth in the market sector for hand and palm print biometrics, with companies proliferating in hardware, software, and services.[36]

These systems claim high accuracy, with one system giving greater than 96% accuracy even against blurred palm images.[37] Still, accuracies have to be interpreted according to the application and the probability of imposters. But since palm prints are easier than fingerprints, if they are indeed sufficiently stable, it would seem to be a very favorable identify verification modality.

### *Iris Scans and Retinal Scans*

The human eye is highly variable across individuals, and certain features are stable over time, thus providing a useful biometric marker. Passports already record eye color, but this provides relatively little specificity across the population.

The pattern of capillaries and blood vessels on the back of the retina (of either eye) can be used as a far more specific biometric. First patented in 1935,[38] the concept was made practical by a device in the mid-1970s,[39] and has since been commercialized and used by government agencies. Since the eyeball must be placed against an eyepiece, and the scan involves low-intensity illumination by an infrared source, the technique is invasive, and only practical for cooperative identification. While spoofing is difficult for this biometric, the retinal pattern can change over time or due to disease or stroke. For this and other reasons, retinal scans for identification have not seen widespread use.

Instead, the iris has proved a more useful biometric. The iris, the annular region surrounding the pupil of the eye which defines the color of the eye, is composed of connective tissue and muscle fibers, and provides a pattern that is specific to the individual. It can even distinguish between identical twins. Proposed in 1936[40] and first patented in the 1980s,[41] an algorithm to perform pattern recognition of irises was licensed to a variety of companies throughout the 1990s.[42] A profusion of different collection methods and matching algorithms have led to increasing practical use, particularly as replacement for physical passports at airport control portals, but proposed for e-commerce and other uses as well.[43] Both theoretically and in laboratory tests, irises are sufficiently variable as to allow unique identification among billions of people.[44]

Iris scans pose challenges to becoming the universal biometric, despite their appealing specificity. While it is possible to obtain an iris scan from several meters away, the optics and collection geometry have to be exquisite, and thus the process is expensive. This is true even for cooperative collection. Mirrored or dark sunglasses and custom textured contact lenses can thwart collection, and eyelashes and reading glasses can get in the way of passive, non-cooperative collection systems.

Still, with improvements in optical systems and digital cameras, as well as faster and more affordable processing capabilities, iris scan technology can be expected to become far more prevalent in the future. Once registered, it provides an excellent way to prove one's identity.

### *Other Modalities*

The field of biometrics is large and growing. Here are some of the biometric fields that weren't discussed above:

- Voiceprints: A spectral decomposition of spoken or recorded speech, plotted as a function of time.
- Typing dynamics: Based on keystroke patterns on a telegraph, computer keyboard, or touchscreen on a smart phone
- Gate and body motion: Style of walking as gleaned from video or smart phones accelerometers, distinctive body motions; patterns of how a device is held
- Body odors: Volatile organic compounds (VOCs) that, for example, dogs can use to identify people
- Chemical effluents: Data from sweat, blood, urine, or analysis of a person's microbiome
- Electrical activity: Electroencephalograms/ Electrocardiographs[45] ("heart prints")
- External physiology: Ear shape, scars, tattoos, periocular and footprint data, and skin reflection

Many modalities can be used in combination to increase specificity. Impersonators can be thwarted if they don't know which combination of modalities will be used for authentication.

## Biometrics Using DNA

The ultimate biometric is one's DNA. Our identity is wrapped up in the 23 chromosomes contained within the nucleus of every cell across our body.[46] These molecules are the core of our identity, and the three billion base pairs contained therein define us as unique individuals based on the many small variations within that code.

Thus, one way to authenticate a person is to sequence their genome and compare the sequence to a pre-stored sequence. While sequencing the entire genome is expensive and time consuming, new solutions that might reduce the cost significantly, and reduce the time required to a mere hour or less.[47]

However, it is not necessary to sequence the entire genome to identify a person. It suffices to find a few dozen locations that vary from individual to individual and sequence those sections alone. This can be done by targeting specific sites, amplifying a few dozen base pairs at each of those locations, and reading off the resulting sequence to obtain identifying information. Currently, forensic DNA analysis uses sites of the human genome with short tandem repeats (STRs), which are specific sites where there are a variable number of repetitions of short sequences of bases where the number of repetitions varies from person to person. A similar approach might also be possible using single nucleotide polymorphisms (SNPs). Using twenty[48] or so such sites (across the chromosome pairs), one can obtain a quite unique identifier of a person, and the process can be accomplished much faster and more economically than sequencing the entire genome.

Sequencing-free genotyping is also being developed. The approach utilizes CRISPR-Cas technologies to precisely target specific sites and then uses biochemical signal generation methods to indicate detection of specific genomic patterns without actually sequencing the region.[49] While still very much in the research stage, these strategies may enable the generation of functionally unique identifiers, while further reducing the time and cost required.[50]

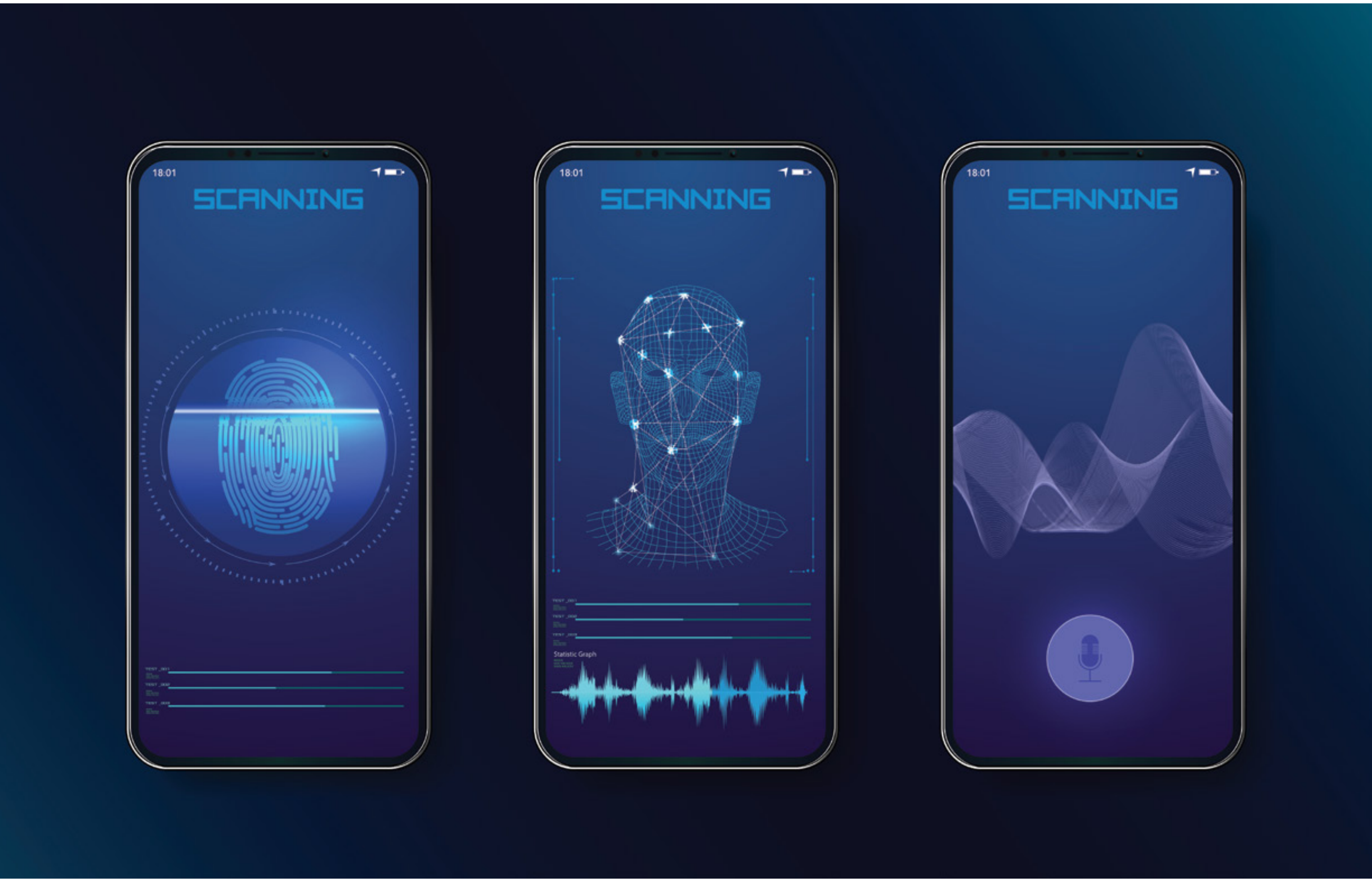
Though there are automated ways of performing sequence and genotype analyses, there are currently no mass-produced affordable analyzers. Further, the chemistry is such that the sequencing of the variable sites will still take a few minutes at least. Thus, DNA biometrics for access control will take too long for most purposes. But for signature verification in place of a notary, say for large purchases or the issuance of passports or other government-IDs, the fact that the verification might take a few minutes (or even an hour) is not a large impediment. After all, signatures are rarely validated in real time. Instead, the challenge is the engineering and production of sufficient numbers of analyzers to make such systems commonplace, and the supply of necessary chemicals.

Indeed, since DNA is the gold standard in identity verification, it is likely that it would be used as the certifying biometric to register other identifiers, which are then used for day-to-day access and verification.

## Conclusion

Given that passwords and multi-factor authentication approaches to authentication are painful and not particularly secure, biometrics offer a better solution. There are many different modalities to choose from, with the possibility of using multiple biometrics to improve specificity. For each modality, there are technical, cultural, and implementation issues. Fingerprint and face recognition technologies have improved but are far from perfect. Retinal and iris scans seem to work quite well, but have not been widely deployed. Other more exotic modalities are not particularly selective. Yet the need to authenticate oneself for security, whether for access or authorization, continues to increase.

Increasingly, there will be a desire to develop non-invasive, non-cooperative biometric capabilities. In this way, authentication can happen without requiring tokens, passwords, credit cards, or other interventions that take time and effort. People can then gain access to a facility or a computer without interruption. They can be authorized to take specific actions based on their identity. Checkout at stores can happen without a chipped credit card. Autonomous ride share vehicles can authenticate their passenger automatically. Health records can be accessed securely. The convenience and security of passive authentication will be compelling for a large variety of audiences and applications.



Since most biometrics are a reflection of one's DNA, and one's DNA is the only truly immutable feature that identifies a person, the ultimate way to authenticate someone is to verify that their DNA matches the registered version of their DNA. Today, this can be done by genotyping or genomic sequencing, which are both relatively lengthy and costly processes. However, in the future, using new technologies, it might be possible to do the verification affordably in minutes. Developing this capability will take research and investment. It will likely take standards to determine the portions of the genome that can be used to distinguish between individuals. It behooves federal agencies to accelerate the development of such capabilities, for both national security and economic dominance applications. The best way to collect a sample for DNA analysis, whether cooperatively or non-cooperatively, remains undetermined. The capability might not come to fruition or might only be used for extraordinary identifications, but the science and technology for DNA-based identification is clear, as are the advantages.

## Endnotes

[1] "The Bertillon System," U.S. National Library of Medicine, April 20, 2021, https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/technologies/bertillon.html.

[2] "Fingerprints: The Convoluted Patterns of Racism." Dickinson College. April 20, 2021, http://dh.dickinson.edu/digitalmuseum/exhibit-artifact/babes-in-the-woods/fingerprints.

[3] Woodrow Wilson Bledsoe, "The Model Method in Facial Recognition," Panoramic Research Inc., Palo Alto, CA, Rep. PR1 15 (47) 1964.

[4] MatthewTurk and Alex Pentland, "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience* 3(1) 1991: 71-86, https://www.face-rec.org/algorithms/PCA/jcn.pdf.

[5] Rajeev Ranjan, et al., "A Fast and Accurate System for Face Detection, Identification, and Verification," *IEEE Transactions on Biometrics, Behavior, and Identity Science* 1(2) 2019: 82-96. https://ieeexplore.ieee.org/document/8680708.

6. Rajeev Ranjan, et al., "Hyperface: A Deep Multi-task Learning Framework for Face Detection, Landmark Localization, Pose Estimation, and Gender Recognition." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 41(1) 2017: 121-135. https://ieeexplore.ieee.org/document/8170321.
7. Sergio Mannino, "Council Post: How Facial Recognition Will Change Retail," *Forbes* May 8, 2020. https://www.forbes.com/sites/forbesbusinesscouncil/2020/05/08/how-facial-recognition-will-change-retail/?sh=19df789f3daa.
8. Aashish Mehra, "Facial Recognition Market Worth $8.5 Billion by 2025." *Markets and Markets* December 2020. https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp.
9. Drew Harwell, "This Facial Recognition Website Can Turn Anyone Into a Cop – Or a Stalker," *The Washington Post*, May 14, 2021, https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/.
10. Sarah Henderson, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software." National Institutes of Standards and Technology, May 18, 2020. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
11. InsafAdjabi, et al., "Past, Present, and Future of Face Recognition: A Review." *Electronics* 9(8) 2020: 1188. https://doi.org/10.3390/electronics9081188.
12. "Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases & Latest News)," *Thales Group* April 10, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition.
13. "Facial Recognition: Top 7 Trends".
14. William Crumpler, "How Accurate Are Facial Recognition Systems – and Why Does It Matter?" Center for Strategic & International Studies, April 14, 2020. https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.
15. "About Face ID Advanced Technology." Apple Inc., February 26, 2020. https://support.apple.com/en-us/HT208108.
16. "Automated Fingerprint Identification System (AFIS) Overview - A Short History," Thales Group, April 5, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history.
17. For instance, IDEMIA's MorphoWave system collects data from four fingers at once. https://www.idemia.com/contactless-fingerprint.
18. "NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech." National Institute of Standards and Technology, May 19, 2020. https://www.nist.gov/news-events/news/2020/05/nist-study-measures-performance-accuracy-contactless-fingerprinting-tech.
19. Alex Hern, "Hacker Fakes German Minister's Fingerprints using Photos of Her Hands." *The Guardian* December 30, 2014, https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.
20. For example, the Center for Identification Technology Research" (CITeR), an NSF Industry-University Cooperative Research Center (IUCRC), and affiliated universities research biometric recognition and credibility assessments. Some of this work features looking at the algorithms for touchless fingerprints. https://iucrc.nsf.gov/centers/achievements/ai-helps-shift-touch-id-to-touchless.
21. William Thompson, et al., "Latent Fingerprint Examination," *AAAS* September 15, 2017. https://www.aaas.org/sites/default/files/reports/Latent%20Fingerprint%20Report%20FINAL%209_14.pdf?i9xGS_EyMHnIPLG6INIUyZb66L5cLdlb; "Report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case." *FBI Forensic Science Communications* 7(1) 2005. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/jan2005/special_report/2005_special_report.htm;Ulery, Bradford T., et al. "Accuracy and reliability of forensic latent fingerprint decisions," *Proceedings of the National Academy of Sciences* 108(19), May 10, 2011. https://www.pnas.org/content/108/19/7733.
22. "'First Signature' Tablet Hits the £140,000 Mark at Bloomsbury Auctions," *Antiques Trade Gazette* July 13, 2020. https://www.antiquestradegazette.com/print-edition/2020/july/2451/news/first-signature-tablet-hits-the-140-000-mark-at-bloomsbury-auctions/.
23. Roger NortonNagel and Rosenfeld, Azriel, "Computer Detection of Freehand Forgeries." *IEEE Transactions on Computers* C-26(09) 1977: 895-905, https://doi.org/10.1109/TC.1977.1674937.
24. Leading researchers in this area include Donato Impedovo & Giuseppe Pirlo, the Central Police University's Department of Forensic Science in Taiwan, CEDAR (Center of Excellence for Document Analysis and Recognition, University at Buffalo, SUNY), and Stanford University's Law and Policy Lab Automated.
25. The leaders in the marketplace include Microsoft Azure, Parascript, ProgressSoft, Biometric Signature ID, Certify Global Inc., and ISign Solutions Inc. See also: "The Signature Verification Market Is Expected to Register a CAGR of 24.77% during the Forecast Period 2019." *Cision PR Newswire* September 11, 2019. https://www.prnewswire.com/news-releases/the-signature-verification-market-is-expected-to-register-a-cagr-of-24-77-during-the-forecast-period-2019--300916140.html.
26. "Signature Verification Market: Growth, Trends, and Forecast (2020 - 2025)." Mordor Intelligence May 12, 2021. https://www.mordorintelligence.com/industry-reports/signature-verification-market.
27. Javier Galbally, et al., "Accuracy Evaluation Of Handwritten Signature Verification: Rethinking The Random-Skilled Forgeries Dichotomy." 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017: 302-310, doi: 10.1109/BTAS.2017.8272711.

28. "Forger Who Duped the Media with Hitler's Diaries," *The Irish Times* February 24, 2013, https://www.irishtimes.com/news/forger-who-duped-the-media-with-hitler-s-diaries-1.1124037.
29. Stephen Mayhew, "Explainer: Hand Geometry Recognition." *Biometric Update* May 13, 2021, https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition.
30. Arun Ross, et al., "A Prototype Hand Geometry-Based Verification System." *Proceedings of 2nd Conference on Audio and Video Based Biometric Person Authentication* 1999: 166–171, http://web.cse.msu.edu/~rossarun/pubs/Ross-Hand_AVBPA99.pdf.
31. Ajay Kumar et al., "Personal Verification Using Palmprint and Hand Geometry Biometric." In: Kittler J., Nixon M.S. (eds) *Audio- and Video-Based Biometric Person Authentication*. AVBPA. Lecture Notes in Computer Science, vol 2688. (Heidelberg: Springer, Berlin) 2003, https://doi.org/10.1007/3-540-44887-X_78.
32. Yingbo Zhao and Ajay Kumar, "Human Identification Using Palm-Vein Images." *IEEE Transactions on Information Forensics and Security* 6(4) 2011: 1259-1274, doi: 10.1109/TIFS.2011.2158423.
33. Kashif Shaheed, et al., "A Systematic Review of Finger Vein Recognition Techniques." *Information* 9(9) 2018: 213, https://doi.org/10.3390/info9090213.
34. J. Svoboda, et al., "Contactless Biometric Hand Geometry Recognition Using a Low-Cost 3d Camera." International Conference on Biometrics, 2015, https://www.semanticscholar.org/paper/Contactless-biometric-hand-geometry-recognition-a-Svoboda-Bronstein/044264a61868bc4e0efb8b501f326cb93f9fade0.
35. Vivek Kanhangad, et al., "A Unified Framework for Contactless Hand Verification." *IEEE Transactions on Information Forensics and Security* 6(3) 2011: 1014-1027, https://doi.org/10.1109/TIFS.2011.2121062.
36. "Palm Recognition Biometrics Market Overview." *Research Nester* February 25, 2021. https://www.researchnester.com/reports/palm-recognition-biometrics-market/2865.
37. Shihab Shawkat et al., "The New Hand Geometry System and Automatic Identification." *Periodicals of Engineering and Natural Sciences* 7(3) 2019: 996-1008, http://pen.ius.edu.ba/index.php/pen/article/viewFile/632/368.
38. Robert B. Hill, "Apparatus and Method for Identifying Individuals through their Retinal Vasculature Patterns." United States Patent, Application Number 759,901, Filed January 17, 1977. https://patents.google.com/patent/US4109237A/en.
39. Robert Hill, "Buzz," "Retina Identification," in *Biometrics: Personal Identification in Networked Society*, ed. Anil K. Jain, et al., ( US: Springer) 1996: 123–41, https://doi.org/10.1007/0-306-47044-6_6.
40. "Modalities." The FBI Biometric Center of Excellence, May 13, 2021. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence-1/modalities-1.
41. Stephen Mayhew, "Explainer: Speaker Recognition," *Biometric Update*. Accessed May 12, 2021, https://www.biometricupdate.com/201206/explainer-iris-recognition.
42. Stephen Mayhew, "Explainer: Speaker Recognition."
43. Luiz Nogueira, "Singapore to Replace Passports with Facial and Iris Detection." *Olhar Digital* October 28, 2020, https://olhardigital.com.br/en/2020/10/28/noticias/singapura-substituira-passaportes-por-deteccao-facial-e-de-iris/?gfetch=2020%2F10%2F28%2Fnews%2Fsingapore-to-replace-passports-with-facial-and-iris-detection%2F; Aaron Brandley, "Next Step in Mobile Security: Iris Recognition," *Epic eCommerce* October 7, 2016, http://epicecommercetools.com/2016/10/07/next-step-in-mobile-security-iris-recognition/.
44. John Daugman, "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons," *Proceedings of the IEEE* 94(11) 2006, https://www.cl.cam.ac.uk/~jgd1000/ProcIEEEnov2006Daugman.pdf.
45. João Ribeiro Pinto, et al., "Towards a Continuous Biometric System Based On Ecg Signals Acquired On The Steering Wheel," *Sensors* 17(10) 2017: 2228, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5676989/.
46. With the notable exception of red blood cells, which are enucleated in mature form.
47. Bradley J. Fikes, "New Machines Can Sequence Human Genome in One Hour, Illumina Announces," *San Diego Union Tribune* January 9, 2017, https://www.sandiegouniontribune.com/business/biotech/sd-me-illumina-novaseq-20170109-story.html#:~:text=Focus%3A%20New%20machines%20can%20sequence,in%20one%20hour%2C%20Illumina%20announces&text=SAN%20FRANCISCO%20%E2%80%94%20DNA%20sequencing%20giant,a%20couple%20of%20years%20ago. May 13, 2021, and https://www.illumina.com.
48. Twenty STR loci are currently maintained in the United States' CODIS database. "CODIS and NDIS Fact Sheet." FBI, June 8, 2016, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet.
49. Sequencing-free testing technologies are being pursued by Mammoth Biosciences (https://mammoth.bio) and Sherlock Biosciences (https://sherlock.bio).
50. Many companies are pursuing biotechnologies related to sequencing and biochemical tests; for a list of several relevant companies, see: Mark Terry, "Top 10 Gene Sequencing Companies by Revenue," *Biospace* Nov 29, 2019, https://www.biospace.com/article/top-10-gene-sequencing-companies-by-revenue/.