NCTA Special Topic:
Emerging Trends in Testing

We are pleased to provide the first JNCTA Special Topic: Emerging Trends in Testing. For this topical section, the focus will be on presenting discussion papers about emerging trends or technologies that are of importance to testing professionals within the testing field. The goal of Emerging Trends in Testing is to increase awareness and stimulate discussion around topics as they are developing and before they become urgent.

The topic for this first Special Topic: Emerging Trends in Testing is Digital Identification. Addressing this topic are three papers: the first paper provides a general overview of Digital IDs, and the subsequent two papers provide commentary on Digital IDs from two highly regarded professionals who specialize in test security and integrity.

We hope that you find this first emerging trend both interesting and informative.

Steve Saladin, Ph.D.
Editor

Journal of the National College Testing Association
2023/Volume 6/Issue 1

The Current State of Digital IDs and Potential Impacts on the Testing Industry

SALLY CARTER, Ed.D.
Southeast Missouri State University

Author Note

Dr. Sally Carter is the Director of Testing Services at Southeast Missouri State University. She has been involved in identification research for eight years, during which time she has conducted workshops, webinars, and presentations. Prior to entering the testing profession, Sally worked as an education specialist with the Missouri NASA Education Program for seven years and spent 12 years as a K-12 educator. She holds B.A. degrees in Speech Communication from Truman State University and Elementary Education from Buena Vista University, and an M.Ed. in Elementary Education and Ed.D. in Educational Leadership from the University of Missouri.

THE CURRENT STATE OF DIGITAL IDS AND POTENTIAL IMPACTS ON THE TESTING INDUSTRY

Our digital world is expanding exponentially. Concepts that seemed improbable a decade ago are now part of our everyday lives. Grocery stores without cashiers, self-driving cars, delivery drones, and cryptocurrency are just a few examples. The evolution of digital wallets can be included in today's digital explosion. Digital wallets store a wide range of information from credit and debit card numbers to store rewards cards, coupons, boarding passes, event tickets, and now, government issued IDs.

Evolution of Digital IDs

Depending on terminology, the history of digital wallets dates either to 1994, with the sale of a CD using an internet credit card transaction (Sacco, 2020), or to 1997, when Coca-Cola allowed vending machine transactions via text (MerchantYard, n.d.). While not true digital wallets, these transactions paved the way for today's advancements. Google launched a true mobile wallet in 2011, and Apple launched Passbook in 2012 (MerchantYard, n.d.). Passbook was the forerunner of today's Apple Pay (Sacco, 2020). Once digital wallets were able to securely process payments, digital IDs became the next goal. Digital IDs refer to both digital driver's licenses (dDL) and mobile driver licenses (mDL). One can assume more acronyms will evolve, since many people do not possess driver licenses and instead use state identifications.

In 2020, the federal government passed the REAL ID Modernization Act, which allowed the Department of Homeland Security to explore accepting digital IDs through the Transportation Security Administration (TSA) (Science and Technology Directorate, 2022). In March of 2022, Arizona became the first U.S. state to offer dDL through Apple Wallet. TSA allows Arizona residents with digital driver licenses to use them as proof of identity at Phoenix's Sky Harbor International Airport (Vigdor, 2022). Maryland became the second state to accept digital driver licenses soon after. TSA currently recognizes mobile IDs at 10 major airports across the U.S. (Transportation Security Administration, n.d.).

The federal government is not alone in the digital ID space. Several states have developed their own apps to manage digital IDs or partnered with a third-party vendor like IDEMIA. At least thirty states have adopted or are considering adopting digital IDs (Velazco, 2022). How exactly are digital driver's licenses developed? Entities developing digital IDs create a digital identity ecosystem. There are three components to such an ecosystem. First, an issuing authority decides to issue a digital ID. This might be a state or federal government, or it could be a school, employer, or other agency. Second, there is the user, the person who needs the ID. Finally, there is the relying party: the agency or company that relies on the authenticity of the ID to grant access and privileges to the ID holder, such as TSA or a bouncer at a bar (Science and Technology Directorate, 2022).

Digital driver license ecosystems are different from apps that store images of IDs. A person can store an image of their ID in their digital wallet in the same way they can store a rewards card or event tickets. A digital ID ecosystem accesses data stored by an issuing authority, informing the relying party as to the validity of the ID. A photo of an ID does not ping back to the issuing authority, and no verification occurs. When the relying party needs proof of identity, there is no need for the user to surrender their device. Instead, a scannable quick-response (QR) code is shown on the user's mobile device. The relying party scans the code using a reader and receives information directly from the issuing authority. The user can customize personally identifiable information, deleting details as appropriate. For example, the bar bouncer does not need to see a user's home address; instead, only their birthdate, photo, and descriptive information such as height and eye color for matching purposes. Well-equipped offices could also require fingerprint matching or utilize facial recognition software to match what the user shows them.

Advantages of Digital IDs

The first benefit of utilizing digital IDs is convenience. People who utilize digital wallets are accustomed to having the ability to store tickets, debit and credit cards, boarding passes, and merchant rewards cards in one location. Adding a legal ID makes sense. An additional convenience is the ability to automatically synchronize information. If you move and need a change of address for your legal ID, you can submit updated information to the DMV electronically. They can verify the new address and update your ID without the need to physically go to their office.

The second benefit of utilizing digital IDs is security. A person would have to use a fingerprint, facial scan, or personal identification number (PIN) to access their digital ID. Proponents argue this will decrease fraud and greatly reduce the number of fake IDs accepted. Issuing authorities also have the capability to erase an ID from a device if the device should be lost or stolen. Lost or stolen devices are locked and potentially can be traced. A lost wallet means anyone who finds the wallet has access to personal information, and wallets typically cannot be traced.

Disadvantages of Digital IDs

Privacy advocates have multiple concerns regarding digital IDs. In many states, it is legal for the Division of Motor Vehicles (DMV) to share data with law enforcement (Velazco, 2022). This could lead to tracking. The American Civil Liberties Union issued a report stating that DMVs could collect information from "every bar, club, casino, office lobby, bank, pharmacy, doctor's office, and airport that you visit" (Stanley, 2021, p. 12). Additional privacy considerations revolve around providing your phone to law enforcement. While the courts have ruled law enforcement does not have the automatic right to search cell phones, there are no clear-cut decisions on what happens if an officer is validating your mobile ID, and a text message pops up that says, "Are you sure you're okay to drive?" or "Don't tell anyone about stealing that stop sign." Does that constitute probable cause for the officer to search you, your car, or your device? Law enforcement officials may not be the only people who can see your personal information. If a hacker gains access to your digital wallet, they would have access to your identification as well.

Since states are developing their own digital ID ecosystems, traveling across state borders could present a problem. You might travel from a digital ID state into a no digital ID state. If you left your physical ID at home, you might not be able to check into your hotel, catch your flight, or prove to law enforcement that you have a valid license. Global implications exist as well. Since each country will develop its own digital ID system, relying parties will have to have the capability of reading international credentials.

Even if you travel within state or to a digital-ID-friendly state, there will be times your phone is not charged, or you do not have good reception. You may have a cracked screen, or you may drop your phone in the pool. Just because you remember your phone more often than your wallet does not necessarily mean more access to your ID. Whoever is reading your digital ID would have to have a working scanner with connectivity back to the issuing authority as well.

Finally, groups are concerned about equity issues regarding Digital IDs. The Pew Research Center (2021) found that 85% of Americans own a smartphone. However, that number drops to 75% for those with less than a high school education, to 76% of those making less than $30,000 per year, and 65% of those over 65 years of age. If possessing a physical ID is equivalent to possessing a digital ID, no equity issues will be present. But what if a venue decides to only accept digital IDs in the future?

Recent Efforts

Some places outside the US have already transitioned to digital IDs. It is important to note that the United States does not require its citizens to obtain a national ID, nor do individual states require residents to obtain IDs (Schultz, 2023). Citizens are issued birth certificates and social security cards, neither of which are valid primary IDs in the testing industry. Many countries outside the United States require all citizens to obtain a national ID at a specific age. State-issued driver licenses are the most common form of ID in the United States. Also, the population size needs to be considered as digital IDs progress. Denmark has a highly successful digital ID, but the entire country has a population of less than six million citizens. The United States has cities and metropolitan areas with larger populations. Each U.S. state has tremendous autonomy when it comes to regulating residents, and many see efforts to formalize a national ID as an invasion of states' rights (Schultz, 2023).

Denmark's digital ID system was instituted in 2010 and was initially comprised of two separate systems, one for government or private service providers and one for banks (*Denmark's Rush to New eID System*, 2022). After more than ten years of use, Denmark announced a major platform upgrade in 2021, integrating the two systems. Denmark's digital system is used for banking, healthcare, legal services such as power of attorney documents, applying for governmental benefits, storing a digital driver license, enrolling children for school, and a messaging service between citizens and public officials. As of September 2021, 95% of the Danish population had in-home access to the internet, 66% of internet users had submitted governmental forms using the digital system, and 91% of system users were satisfied with how easy it was to use digital services (Agency for Digital Government, 2021). Overall, Denmark's digital system is meeting the needs of its citizens. People download the app, and their governmental and banking services are available in one location. However, even with the success of the current system, there are concerns surrounding the system upgrade.

Denmark's system works by creating a code that verifies identity (*Denmark's Rush to New eID System*, 2022). Danes are required to use codes for online purchases. The old system allowed people who did not have a smartphone or did not want to download the app to use alternate methods of proving their ID. The government published a physical code book and issued hand-held QR code generators. The new Danish digital system will have alternatives, but they are not yet available. People without a smartphone can still use the old system for now. The old system is scheduled to be completely phased out by June 2023. Advocacy groups are concerned that marginalized populations might have problems accessing necessities.

Denmark's success is encouraging, but some efforts have not been as successful. New South Wales, Australia, implemented a digital driver's license in 2019. According to ServiceNSW, the governmental agency responsible for the licenses, the new digital ID would "provide additional levels of security and protection against identity fraud, compared to the plastic [driver's license]" (Goodin, 2022, para. 1). However, using an ordinary computer and an easily available PIN breaker, ServiceNSW IDs can be forged in under an hour by people with relatively little computer expertise. There are videos on YouTube showing people how to change personally identifiable information on their digital IDs in less than one minute. Goodin (2022) lists major security flaws in the IDs including lack of adequate encryption; the fact that data is never validated by an issuing authority; the pull-to-refresh function only updating the QR code, not the ID itself; the QR code not being validated when scanned by a relying party; and the fact that the app allows stored data to be backed up and restored, since the backup data can be manipulated before restoring information to the ID. A person can change their name, address, and birthdate in the app-generated code with little effort. It does not change the information on the ID, but they are not showing the actual ID, just an app-generated code.

Digital IDs and the Testing Industry

As digital ID technology advances, the testing industry needs to be forward-thinking. Adoption of digital IDs has been slow, which allows time for policy development. But this should not be construed as permission to wait and see what happens. Instead, a proactive approach is needed.

First, test sponsors, providers, and testing center personnel need to develop standards and guidelines on how to authenticate and accept digital IDs. Standards and guidelines need to be inclusive of the various state ID platforms. Is the standard going to be that test centers accept all forms of digital IDs, only digital IDs from the test center's state, or perhaps the testing industry decides only physical IDs will be accepted without exception? Specialized equipment may need to be purchased or developed to prevent proxy testing. Digital ID proponents are quick to point to biometric or PIN security, but both are easily bypassed. Anyone's fingerprint can be added to smartphone security settings, and the sharing of PINs and passwords already happens.

Second, the testing industry needs to embrace the opportunity for increased exam security through digital IDs. True digital ID systems that ping information from a government source provide a level of security against fake IDs that the inspection of physical ID cards does not provide. Apps like Show-Me ID, developed by the Missouri Division of Alcohol and Tobacco Control (2021), can detect expired IDs and can notify the user if a scanned ID is problematic and a possible fake. The app does not store ID scans or personally identifying information. While developed to help deter underage drinking, similar apps could be designed for use in the testing industry.

Finally, testing professionals need an active voice as digital IDs are developed. A QR code yielding a name and date of birth is not enough to prove identity for seating test takers. A recent photo and signatures are needed for on-site matching. Assurances need to be made that every state-developed digital ID does not merely display a photo of a stored ID, but also includes verification from an issuing authority. If it is easy to store a genuine ID, concert ticket, or purchase receipt in a digital wallet, it is easy to store a fake as well. Safeguards are critical.

The emergence of digital IDs represents a significant technological advancement with profound implications for the testing industry. Specific requirements and concerns shared across the testing industry should be actively discussed with policy makers and product developers. Ensuring the needs of the testing industry are addressed will be critical to meet industry standards of candidate verification and test security.

REFERENCES

Agency for Digital Government. (2021, September 1). *Numbers and statistics*. Ministry of Digital Government and Gender Equality. https://en.digst.dk/numbers-and-statistics

Goodin, D. (2022, May 24). *"Tough to forge" digital driver's license is... easy to forge*. Ars Technica. https://arstechnica.com/information-technology/2022/05/digital-drivers-license-used-by-4m-australians-is-a-snap-to-forge/

MerchantYard. (n.d.). *The history of e-wallet*. https://www.merchantyard.com/blog/the-history-of-e-wallet

Missouri Division of Alcohol and Tobacco Control. (2021, April 1). *New app from Missouri Division of Alcohol and Tobacco Control allows retail cashiers to verify authenticity of IDs with their phones*. Missouri Department of Public Safety. https://atc.dps.mo.gov/news/newsitem/uuid/92b716c5-ecb1-46f7-8409-b66cd49301d6

Denmark's rush to new eID system could leave online shoppers starving. (2022, September 21). Mobile ID World. https://mobileidworld.com/denmarks-rush-to-new-eid-system-could-leave-online-shoppers-starving-409211/

Pew Research Center. (2021, April 7). *Mobile fact sheet*. https://www.pewresearch.org/internet/fact-sheet/mobile/

Sacco, F. (2020, September 29). *The history of digital wallets*. 7 17 Credit Union Financial Fundamentals Blog. https://blog.717cu.com/resources/education/financial-education-blog/the-history-of-digital-wallets

Schultz, D. (2023, November 22). *National identification cards*. The Free Speech Center at Middle Tennessee State University. https://firstamendment.mtsu.edu/article/national-identification-cards/

Stanley, J. (2021, May). *Identity crisis: What digital driver's licenses could mean for privacy, equity, and freedom*. American Civil Liberties Union. https://www.aclu.org/sites/default/files/field_document/20210913-digitallicense.pdf

Science and Technology Directorate. (2022, January 31). *Next generation identity: Mobile driver's license fact sheet*. U.S. Department of Homeland Security. https://www.dhs.gov/science-and-technology/publication/next-generation-identity-mobile-drivers-license-fact-sheet

Transportation Security Administration. (n.d.). *When will the phased digital ID rollout start? Which airports/states will be first in line for this new technology?* U.S. Department of Homeland Security. https://www.tsa.gov/travel/frequently-asked-questions/when-will-phased-digital-id-rollout-start-which-airportsstates

Velazco, C. (2022, March 24). *Digital driver's licenses take the sting out of forgetting your wallet. Here's how they work*. The Washington Post. https://www.washingtonpost.com/technology/2021/10/11/digital-drivers-license-mdl/

Vigdor, N. (2022, March 26). *Arizona offers driver's licenses on iPhones. Other states want to be next*. The New York Times. https://www.nytimes.com/2022/03/26/us/arizona-digital-drivers-license.html

How Digital IDs Can Both Help and Harm the Testing Industry

RAY NICOSIA, M.A.
Educational Testing Service

Author Note

Ray Nicosia is the Principal, Test Security for Educational Testing Service (ETS). He researches, establishes, and coordinates test security policies for ETS and oversees investigations for the Chief Security Office. Test security policy includes all high stakes paper- and computer-based testing programs for ETS at 25,000 test centers across 192 countries, as well as through the At Home delivery process. As the longest tenured testing official in the industry, Mr. Nicosia is recognized as the leader in the business, implementing multiple prevention and detection test security techniques to better serve ETS and its clients. His investigations have resulted in actions taken by federal and local law enforcement agencies, civil prosecutions, and the closings of test centers. Mr. Nicosia has audited more than 700 test centers and has testified in court internationally and domestically. He is frequently quoted by the media as an expert in academic integrity issues and has represented ETS in business development matters on six continents. Mr. Nicosia joined ETS in 1989. He holds a master's degree in Business and Organizational Security Management from Webster University and a B.A. from William Paterson University.

HOW DIGITAL IDS CAN BOTH HELP AND HARM THE TESTING INDUSTRY

According to The World Bank (Clark et al., 2023), 850 million people globally do not have any form of identification (ID). This is a staggering but perhaps not surprising figure.

For hundreds of millions around the globe, lacking even a basic form of ID, let alone a digital ID, all but closes the door to any shred of opportunity that could be made available, including access to a high-quality education. As we continue to witness the acceleration of technology and digitization, the need to keep up with trends in digital IDs becomes even more important.

The educational assessment industry has long relied on reliable forms of identification to deliver products and services both in the U.S. and around the globe. Educational Testing Service (ETS) is no exception. Prior to the pandemic, when test center testing was the primary delivery method for our tests in over 200 countries around the world, verifying test taker identities was a critical part of our test security process. Even with the prominence of remote testing today, knowing that a test taker who registered for an exam is the same person sitting behind the computer screen is a key part of our security protocol.

With the pace of technology today, the rise of digital IDs can both help and harm the testing industry. Here's why.

How It Can Help

Properly identifying test takers across the globe is critical to ensuring everyone is given the correct exam under appropriately authorized circumstances. This is foundational to providing exam security. With the rise of digital IDs, the convenience of being able to consistently carry a valid form of identification becomes all the more prevalent.

Allowing digital IDs to be accepted for test administration is not only convenient for test takers but also for test centers. Our goal is consistently finding new and different ways to streamline our processes and make the verification process easier without sacrificing security. Digital IDs can be one way to do that. Although they are a useful alternative to traditional IDs, they do come with some challenges and could do more harm than good in the short term.

How It Can Harm

A common standard in the assessment industry is that a test taker maintains possession of their ID throughout their test so that it can be checked after scheduled and unscheduled breaks. Having an ID visible at a test taker's workstation during testing also allows proctors to confirm the right test taker is in the right seat, taking the test assigned to them.

The rise of digital IDs, which can be commonly accessed and carried on cell phones, is complicated by the policy that test takers are not permitted to use or access their phone during their test session. Cell phones have, over many years, been used to cheat by removing test content from an exam and sharing it with others, bringing in answer keys, and communicating with others during the testing process. While convenient in being accessible via cell phone, digital IDs do come with this added complication.

To this end, in August 2022, ETS studied the use of digital IDs in South Korea, where acceptance of a digital ID is mandated by law. At test centers throughout the country, staff were trained on how to handle test takers who showed up to their testing appointments with digital IDs.

In the presence of the proctor, test takers can present their digital ID via a government web site on their cell phones. Notably, the ID is not maintained in static form, such as a screen shot. Testing staff observe the proper web site is accessed (i.e., not an artificial, duplicate site), and just as they would be in the standard verification process when a passport is presented, the photo and name on the digital ID are compared to the test taker and the name on the test registration.

ETS process then mandates a new, real-time photo of the test taker to be taken. As an additional tool to combat impersonation, ETS captures a voice sample of Test of English as a Foreign Language (TOEFL), Graduate Record Examination (GRE), and Praxis test takers. After the check-in process is completed, the same phone security protocol is followed, where the test taker must place their phone in a secure location, such as a locker. Test takers are then checked with a hand-held metal detector to ensure they do not have a second phone or other form of digital device.

The test taker is then escorted from the check-in station to their workstation by testing staff. The photo of the test taker just captured is displayed on the workstation computer. Should the test taker remain seated at their workstation throughout the assessment, there is little need for an ID check. However, should the test taker need an unscheduled break, testing staff are instructed to pull up the photo of the test taker taken at check-in and compare it to the person attempting to return to the testing room and specific workstation.

While most test takers in South Korea continue to present physical IDs, some have presented their digital IDs. During ETS' pilot period, with a limited sample, testing staff reported no issues. No concerns were raised about the additional few moments it takes to pull up the photo on the check-in computer when test takers return from a break.

While digital IDs are certainly a more accessible avenue to verify a test taker's identity, they come with some drawbacks. One of those drawbacks is the lack of standardization. This presents significant difficulty as globally, each country will inevitably design and format their IDs differently. We will likely see the same occur domestically in the U.S. as well.

Keeping up with these trends, knowing what to look for, and training proctors and test center administrators on evolving formats will present challenges as digital IDs become more commonplace. While technology and digitization are inevitable, this opens the door to more opportunities for fake IDs to be created and duplicated, increasing the potential for identity theft and impersonation.

REFERENCE

Clark, J., Metz, A., & Casher, C. (2023, February 6). *850 million people globally don't have ID—why this matters and what we can do about it*. World Bank. https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about

A Technological Alternative to Identification Documents in Test Taker Authorization

DAVID FOSTER, Ph.D.
Caveon

Author Note

From 1990-1997, David directed certification test development for a certification program at Novell, a networking software company, where he introduced computerized adaptive testing on a worldwide scale, pioneered new item types, and launched simulation-based testing. Following his tenure with Novell, he co-founded Galton Technologies to provide test development technology and services to certification programs. In 2003, David co-founded the industry's first test security company, Caveon. Under his guidance, Caveon has created new security tools, analyses, and services to protect exams. Amid rising concerns about fairness in testing, David has focused on changing the design of items and tests to reduce the harmful effects of cheating and testwiseness. He has served on numerous boards and committees over the years, including those associated with ATP, ANSI, COTS, and ITC. He also founded the Performance Testing Council to raise awareness of the principles required for quality skill measurement. He has authored numerous articles for industry publications and journals and has presented extensively at conferences. David graduated from Brigham Young University in 1977 with a Ph.D. in Experimental Psychology. He completed a post-doctoral fellowship at Florida State University in 1981.

A TECHNOLOGICAL ALTERNATIVE TO IDENTIFICATION DOCUMENTS IN TEST TAKER AUTHORIZATION

Today, the most common way to verify that a person is authorized to take a high-stakes test begins with requiring the display of a form of official identification (ID), such as a government-issued driver's license or passport. Under some conditions, a school-issued student ID will suffice for tests that are given in secondary school or college. The logic is that such a document verifies a person's identity, and if that person has scheduled to take a test at a center or online, and the schedule includes the same name and other identifying information, then they are allowed to proceed. In the past and as a current practice, these identification documents have been physical, usually on paper or plastic. There is a growing trend for such documentation to evolve to exist only in digital form. A digital ID is one that might be on a phone or tablet and displayed on the screen. It may be accompanied or supported by other forms of security, such as digital signatures, photographs, passwords, and biometrics.

One risk of ID documents, whether digital or physical, is that they can be faked, and that faked ID might be sufficient to allow a person to take an important test on behalf of another. This is called proxy testing, and it has been a common and successful cheating practice for decades. The better the fake ID, the more likely the effort to cheat will be successful. With today's high-quality printing and digital technologies, it is easier than ever to create these fakes.

Using one or more biometrics is another way to verify a person's authorization to access a system, such as a testing system. Examples of this type of authorization are the different biometrics I use to access my phone and tablet. As an example, my phone uses facial recognition, and my tablet uses fingerprints. When I initially bought these devices, during the setup process, I provided these biometrics by following a few simple steps. Since then, several years later, these biometrics have consistently allowed me to access and use these devices, while at the same time preventing anyone else from doing so. The authentication process in each case is simple, mostly automatic. For my phone, the process is activated when I pick it up, recognizing my face automatically and giving me access to all the phone's functions immediately. For my tablet, I need to simply do an initial step of placing my finger on the reader to activate the process. Almost as quickly as the phone, I am able to use the tablet.

Identification Versus Authentication

The preceding section illustrates the essential differences between the processes of identification and authentication. First, the goal of the former is to confirm the identity of the person seeking to take an exam, as a first step in verifying their authorization to do so. This is done by viewing a document that contains relevant information and matching that information to the person presenting it (e.g., picture, signature) and to information contained on the testing schedule (e.g., name, date of birth). A passport or driver's license provides the data for matching, and thus, proof of that identity. For authentication, establishing identity at the time of testing as a separate process is irrelevant. It simply assumes that the testing program that published the test has already collected identity information to suit their purposes, and that that identity has been linked to a biometric. The authentication process has the simple goal of matching the biometric established at an initial sign-up, scheduling, or registration event with the biometric provided just prior to the scheduled exam. To recap, an identification process strives to establish the identity of the test taker in order to verify authorization to test, while the authentication process simply verifies the authorization to test, without a separate process of establishing identity.

A second difference is that the identification procedure relies on the comparison of a physical (or digital) identification document that has been validated by an issuing authority with an individual and/or other sources of information. That document may be captured and stored as part of the data for a testing event. While this process is subject to human error, it does not typically rely heavily on technology. In contrast, the authentication procedure is less prone to human error but does rely more heavily on technology. It requires first that a current biometric be easily provided upon request, and second, the testing system is capable of immediately comparing that biometric against the source biometric created earlier in time. With the internet, it would be possible to confirm a match or non-match on a local server even if the source biometric were housed at a distant server.

As a third difference, the identification process is more complex and time-consuming, perhaps made even more complex with digital IDs. Several steps are involved in handling the ID, reviewing and attempting to verify the legitimacy of the ID, eventually taking a picture of the ID, and finally making a decision as to whether to allow the test taker to proceed and take the test. In contrast, providing a biometric is a simple step, built into the technology and prompted by the technology, and verified quickly, also by the technology. Human involvement or intervention is mostly unnecessary when processing biometrics and making authorization decisions.

A final difference has to do with privacy concerns, particularly the protection of personally identifying information (PII). There are high standards throughout the world concerning taking great care with PII. A process relying on establishing identity will involve the display and capture of identifying information, with individuals like proctors being privy to that information. With a biometric authentication process, the PII was captured at registration, and it is not necessary to continue to disclose it to third parties. For the purposes of testing, personnel at testing centers, or the test administration software itself, may never need to be aware of the PII of the test taker. In extremis, test takers could be assigned a temporary authorization code that would not even require them to disclose their name.

Two Main Types of Authentication Processes:

One to One. The simpler form of authentication is to compare a biometric provided at an earlier time to one provided when requested before being allowed to take a test. This is how access to my phone works. When I pick up the phone, it automatically compares my face now with my face when I bought the phone. So far, this system has been working flawlessly for years. The same process occurs for anyone else picking up my phone, but the result is that their access is denied.

One to Many. This form of authentication involves matching an obtained biometric with every biometric entry in a larger database. Police fingerprint detection analyses work this way. All they have is a fingerprint and a database of perhaps millions of fingerprints. The system must compare the obtained fingerprint against all the other fingerprints until they find a match. A one-to-many match is not an inherent quality of the biometric, but rather of how it is used. My fingerprint biometric which works on my tablet as a one-to-one match could also be used by the police in a one-to-many search.

It is important to understand that for the authentication of students or adults in the workplace to take a test, a one-to-one match is quick and safe. A one-to-many matching process, which by its nature raises privacy concerns, is not needed.

Types of Biometrics

The World Bank (2019) provides a very useful practitioner's guide to biometrics. They describe that there are two general types of biometrics: behavioral and biological. The former are biometrics about the behavior of a person (e.g., how they walk, how they talk, how fast they type on a keyboard, and many others). The physical or biological biometrics record and evaluate a person's physical features (e.g., facial structure, fingerprint, or patterns of blood vessels in the eye or palm, to list a few).

The World Bank (2019) also compares some biological biometrics in terms of cost, equipment needed, disadvantages and advantages and several other important qualities. Unfortunately, there are currently no biological biometrics that are relatively inexpensive and easy to use that also offer a high degree of accuracy.

In my experience there may be more behavioral biometrics available for use or ones that could be developed. One example that has seen some use in the testing field is keystroke analysis. For this biometric, the prospective test taker is asked to type a phrase, perhaps the same phrase that was typed at the registration process. The computer calculates the dwell time (i.e., how long a person stays in contact with a key) and the flight time (how long the interval is between leaving contact with one key and contacting another key) for dozens of keys pressed when typing a phrase. The pattern of those times would provide a unique biometric for a person, because everyone types differently. The use of the keystroke analysis biometric may or may not work well for a particular test-taking audience and may have a list of advantages and disadvantages. A testing program wishing to make use of a behavioral biometric would need to either select or develop one and would need to require that individuals involved in online or onsite test administration be able to collect and compare that specific biometric.

Regardless of the biometric, behavioral or biological, there are a number of issues that need to be considered prior to implementation. Here is an incomplete list of principles of biometrics use for authentication to take tests that are worth considering.

1. Biometrics should be hardware independent when possible.
2. Biometrics should not be the same as those used for government identification purposes.
3. Biometrics should work well independent of cultural, ethnic, or racial differences.
4. Biometrics should accommodate individuals of all ages, genders, disabilities, and other identity categories.
5. More than one biometric may need to be available and offered.

6. Biometrics for authenticating test takers should use one-to-one matching instead of one-to-many matching.
7. Biometric data should be protected when stored or transferred and should present no risk or do no harm if the biometric data were stolen and disclosed.

Summary

This paper recommends learning about and considering the use of an authentication procedure in addition to or as a replacement for identification-based authorization procedure. In its simplest form, the authentication procedure involves the one-to-one matching of a biometric collected at the time of scheduling or registration with the same biometric provided just prior to being allowed to take a test. If the two match, the testing can move forward. Authentication procedures may be easier to perform, may solve more of the issues concerning the use of digital IDs, may be less expensive to use, may be more protective of PII, and may avoid other problems inherent with a system that relies on the identification of the test taker.

REFERENCE

World Bank. (2019, October). Biometric data. In *ID4D Practitioner's Guide: Version 1.0*. (pp 122-128). https://id4d.worldbank.org/guide/biometric-data