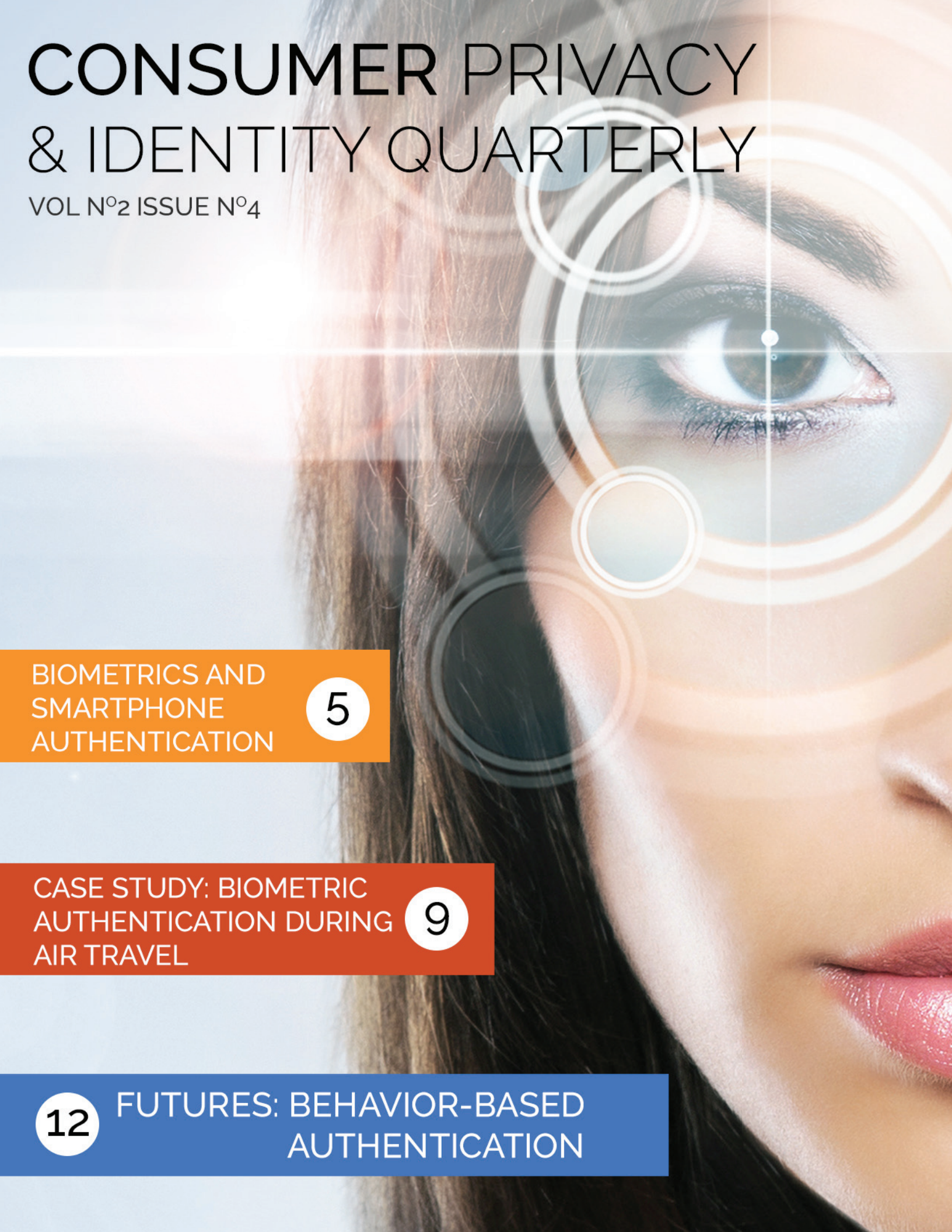
# CONSUMER PRIVACY & IDENTITY QUARTERLY

VOL N°2 ISSUE N°4




# DISCLAIMER

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

FOR MORE INFORMATION OR QUESTIONS EMAIL osd.ncr.osd.mbx.dodsmartcards@mail.mil

# IN THIS ISSUE:





# ALSO INSIDE:





# INTRODUCTION: BIOMETRIC AUTHENTICATION METHODS & PRIVACY

*"In a world of biometric security, you are the password."*

How often do you open your inbox to find an email from a major financial or Social Networking Service (SNS) provider with the subject line "URGENT: Reset Your Password?" If you are one of the 143 million consumers impacted by the Equifax data breach of September 2017, or one of the four million DoD employees impacted by the Office of Personnel Management (OPM) data breach in 2015, you probably received similar emails in recent memory.

In the wake of devastating personal information leaks such as these, in which millions of username and password combinations were compromised, questions are raised concerning the ubiquity of passwords as the primary digital authentication method. After all, passwords have obvious vulnerabilities that already plague consumers. They are easy to crack, hard to remember, and require changing every time a data breach occurs.

As an alternative solution, biometrics are being used in place of passwords to authenticate users across consumer applications and devices. Biometrics are distinctive, measurable physical and behavioral characteristics used to describe and identify individuals. Physical characteristics relate to the shape of the body, whereas behavioral characteristics relate to the pattern of a person's activities, such as typing rhythm or gait. Biometric authentication looks at these features for identification or access control purposes. Some systems recognize faces or fingerprints—the two most popular modalities for identification. Others recognize voices, irises, or even heartbeats. Biometric systems are increasingly being built into mobile phones, wearable devices, and cloud-based apps to create a password-free login experience, transforming your body into the password.

But are biometrics really more secure than passwords? Both methods offer strengths and weaknesses that make each suitable for different scenarios. However, the buzz surrounding biometrics is high today, as more products using biometrics technology are being released. For instance, Facebook uses face recognition to find and group photos of a person for easy tagging, Apple's Touch ID uses fingerprint to grant users device access, and Snapchat's popular face effects are powered by its real-time detection algorithms. It's no surprise that biometric authentication is gaining traction as consumers grow comfortable with scanning and sharing biometric data in everyday contexts.

This CPIQ issue investigates the rise of biometric authentication methods across multiple consumer use cases and analyzes the privacy implications and risks that accompany this technology. The feature explains how biometrics are used for authentication in mobile devices, why biometric authentication applications are on the rise, and the basic biometric concepts necessary to understand how your bodily data is stored and exploited for identification. Next, we analyze how biometric authentication is disrupting 1) how you bank online, and 2) how you travel by air. The next two articles examine existing biometric data safeguarding practices and assess their strengths and weaknesses against hacks and malicious attacks. Lastly, we zoom in on behavioral biometrics, the next frontier in biometric authentication.

With pushes from hardware manufacturers like Apple and Samsung, both releasing devices with built-in biometric authentication systems, it seems only a matter of time before biometrics replace passwords to become the preferred authentication method for mobile and device access. Read on to prepare yourself for the upcoming changes in how we digitally register and verify our identities online.

*NEXT: Biometrics and Smartphone Authentication*

# BIOMETRICS AND SMARTPHONE AUTHENTICATION

Increasingly, smartphone producers are using biometrics to allow users to unlock smartphones and verify their identities before downloading apps and making purchases. Biometric authentication methods, when used together with other traditional authentication methods, provide users with enhanced security. The newest generation of smartphones, such as the iPhone X, use novel biometric technologies in conjunction with traditional passwords to authenticate users and protect their data.

## Biometrics and Smartphones

By the early 2010s, smartphone producers understood traditional alphanumeric passwords were becoming easier for hackers and other malicious individuals to steal and crack using sophisticated techniques; often hackers could steal a user's password from an online service and then use it to gain access to other services and physical devices. Some hackers began using dictionary attacks and other brute force methods to crack passwords. These techniques allowed hackers to cycle through thousands of different alphanumeric combinations trying to find a user's password.

To counter the weaknesses of passwords and increase convenience for consumers, smartphone producers turned to biometrics. Unlike passwords, which can be stolen and reused by anyone who knows them, biometrics rely upon a user's physical attributes and behavior to provide access to a device. In contrast to passwords, biometrics are difficult to steal and reuse. Biometrics give users increased security when accessing their smartphones and when authenticating to download apps and make purchases on smartphones.

## The Most Commonly Used Biometric Modalities

The most common method of smartphone biometric authentication is fingerprint recognition. Fingerprints belonging to one individual rarely falsely match those belonging to another; this makes fingerprints a relatively strong and convenient biometric to use for authentication and identity verification. For example, Apple claims their fingerprint recognition system used on iPhones, TouchID, has a one in 50,000 chance of mistaking a random finger for the registered user's finger. Two of the earliest smartphones to use fingerprint recognition technology were the Motorola Atrix 4G in 2011 and the iPhone 5S in 2013.

Face recognition is emerging as a convenient new modality for smartphone authentication. Apple's release of the sophisticated face recognition system, Face ID, for the iPhone X may signal the increasing use of face recognition for smartphone authentication. Like fingerprints, almost all individuals have unique facial features which can be used for secure authentication. For example, Apple claims the Face ID system used on the new iPhone X has a one in 1,000,000 chance of mistaking a random face for the registered user's face.

Some smartphone producers have experimented with other biometric recognition systems which rely on iris recognition and behavioral characteristics. The Samsung Pass, a biometric authentication app for Samsung smartphones, allows users to authenticate through iris recognition in addition to more traditional modalities. Some technology producers have experimented with the use of behavioral recognition techniques for smartphone authentication. However, smartphone producers have not widely adopted behavioral authentication techniques as of this issue's publication.

*Continues on Page 6...*

## The iPhone X and Face ID

The iPhone X uses a sophisticated new face recognition system, called Face ID, to allow users to unlock the device and authenticate before downloading apps and making purchases. The Face ID system replaces the Touch ID fingerprint system used on previous versions of the iPhone (since the release of the iPhone 5s in 2013). The optional authentication system allows users to unlock their iPhone by simply glancing at the front iPhone camera. Face ID works in the dark, in low lighting conditions, and automatically adjusts to take into account changes to the user's face caused by makeup, facial hair, and other common factors.

Face ID does not replace traditional alphanumeric passcodes on the new iPhone, but instead works in conjunction with them to provide higher security. In most cases, if the user decides to enable Face ID and the system detects the user's face, it will allow the user to access the Phone X without presenting a passcode. However, users are still required to present their passwords in some instances to prove their identity. For example, if the device has been restarted or just turned on, the device has not been unlocked for more than 48 hours, or if the user fails to unlock the device five times using his or her face, the user will have to enter a password.

## Vulnerabilities and Countermeasures

Despite the increased security provided by biometric authentication methods, hackers have still managed to develop techniques to spoof and fool smartphone biometric authentication systems. Spoofing techniques, where hackers copy or make artificial biometric signatures, sometimes allow them to illicitly gain access to smartphones protected by biometric authentication.

To increase the security of smartphone biometric authentication, smartphone producers turned to anti-spoofing countermeasures to ensure only the real biometrics belonging to the owner of a smartphone would be sufficient for authentication. One of the most important smartphone anti-spoofing methods is liveness detection. Liveness detection is a technique used to verify whether a user is presenting a real, "living" biometric to verify his or her identity.

Modern biometric authentication systems include sophisticated liveness detection to deter spoofing. Some liveness detection techniques work by checking to see whether the biometric presented by the user conducts electricity like a living human being. Other methods verify whether

### PASSWORDS VS. BIOMETRIC AUTHENTICATION
### A BREAKDOWN

Are biometrics really better than passwords? It's a question most consumers have wondered as more devices and applications use biometric authentication. Here's an honest breakdown of biometrics and passwords' strengths and weaknesses by security and convenience.

= biometrics = passwords

*Note: both icons = TIE between password & biometrics

| | PASSWORDS | BIOMETRICS | WINNER |
|---|---|---|---|
| Ease of Use | Easy to use, just requires the user to provide a username and password | Easy to use, just requires user to present biometrics | * |
| Ease to Deploy | Simple and inexpensive to deploy, no extra configurations required | Initial cost is high for deploying biometric systems requires additional hardware & software for biometrics collection and matching | |
| Multiple Identity Checkpoints During Authentication | Does not provide strong identity checks, as it is only based on matching a password | Biometrics allow for multiple identity checkpoints, such as liveness detection or multi-factor authentication | |
| Ability to Forget | Easy to forget passwords | Users cannot forget biometrics | |
| Vulnerability to Hacking and Spoofing | Easy for hackers to crack and exploit with computational advances | Spoofing biometrics is often more difficult than hacking a password | |
| Susceptibility to User Error | Users can incorrectly enter passwords and make typos | Users cannot make typos when providing biometrics and generally commonly used biometrics are easy to present to sensors | |
| Need to Change Frequently | Users have to change passwords frequently | Users do not need to change biometrics | |
| Contingency in the Event of a Breach | Users can change their passwords, little personally identifying info is revealed | Biometrics cannot be changed & may reveal identity info such as face images or fingerprints | |
| Existing History of Data breaches | Many usernames and passwords have already been compromised in previous data breaches | Biometrics breaches have occurred & are likely to become increasingly common | * |
| Error Rates | If entered correctly, passwords almost always work | Matching algorithm isn't 100% accurate, "false positive" or "false negatives" can occur | |
| User Comfort | Generally, users are comfortable providing a user ID and password | Some users feel uncomfortable providing biometrics for privacy reasons | |
| Susceptibility to Environmental Factors | Works in all environments | Environmental factors, such as noise level and lighting, and sensor state can make authentication difficult | |

So who wins? Biometrics is ideal for authentication systems where security is the utmost concern, whereas passwords might be better suited for deployers who want a simple, low-cost solution. In either case, using multi-factor authentication will provide the maximum possible protection.

*Concludes on Page 7...*

a person's face makes small, naturally occurring movements when looking at a camera. Other anti-spoofing techniques make three-dimensional models of a user's face to ensure the user is not presenting a photo of another person's face for authentication.

The new iPhone X Face ID system uses sophisticated anti-spoofing techniques to protect users. Face ID utilizes a proprietary TrueDepth camera on the front of the iPhone X which projects more than 30,000 invisible infrared dots onto the user's face to map its structure. Face ID detects the direction of the user's gaze and uses neural networks to match the user's face and deter spoofing.

### Conclusion

Smartphone producers are increasingly turning to biometric authentication methods to protect their devices. Biometric authentication methods, although susceptible to some sophisticated spoofing techniques, provide a higher degree of security than traditional alphanumeric passwords. The smartphone industry should continue to combine sophisticated biometric authentication techniques along with anti-spoofing countermeasures in conjunction with traditional passwords to protect consumers.

# CASE STUDY: BIOMETRIC AUTHENTICATION IN EVERYDAY FINANCIAL TRANSACTIONS

The financial industry—including traditional and online banks and mobile wallet providers—has begun to include biometric authentication as a part of everyday user interaction. Here is a look at how your everyday transactions may include authenticating with your biometric data.

### Mobile Banking

Smartphones have allowed us to access apps and features on the go, so looking how we handle our money with them is critical. Mobile transactions have incorporated fingerprint authentication for some time through Apple's Touch ID. Touch ID is essential to apps such as ApplePay and Amazon, which require the scanning of a user's fingerprint to authorize payments and access the entirety of offered services. Mobile wallets such as PayPal and Venmo also use TouchID for sign-in and purchase verifications.

Eye scans are gaining traction as a biometric authentication method in mobile banking. Wells Fargo uses EyePrint ID by EyeVerify for user authentication and login. EyePrint ID focuses on the micro details and veins in the whites of

*Concludes on Page 8...*

the eyes instead of traditional iris detection or iris scanning. Traditional iris scans require a near-infrared camera to function whereas EyePrint ID just requires the standard front-facing lens available in most smartphones.

### Online Banking

Even though your handheld devices allow access to apps and mobile sites, they lack the full layout and functionality you access on websites using computers. In online banking, you can now use facial recognition to confirm your identity and sign into accounts instead of passwords. Lloyds Banking Group has rolled out facial recognition authentication for customers with Windows 10 devices. The Windows 10 "Hello" software combined with Microsoft hardware creates a data representation of a user's face for comparison instead of an image. Currently in the trial stage, the software uses infrared technology and liveness detection to authenticate users for online access.

### Phone Banking

Although we conduct most financial transactions digitally, some transactions still require talking to an actual person in person or via phone. Voiceprint authentication is a popular method to verify users over the phone. Voiceprint captures the unique quality of your voice, both the tone created by your vocal cords and folds and the environmental aspect created by accents, regional dialects, and the way your mouth moves to create sounds.

Barclay's, a UK-based financial services company, uses voiceprint authentication for call center interactions. Barclay's Voice Security uses Nuance FreeSpeech to record an automatic voiceprint when users call for the first time; call center personnel then ask whether users would like to enroll in the service. Connecting the voice print to the account requires relaying the user's account number and confirming identification. Once set up, every time the user calls in, the voice print is used to confirm identity. If users do not want to enroll in Voice Security or wish to opt out, Barclay's will remove the voice print and will not create a new one until the user requests it.

### Conclusion

You may be concerned about the security implications as the financial industry continues to implement biometric authentication methods. Biometric solutions offer additional account protection and security to the everyday user, even if the idea of sharing such data makes you wary. Your transactions are most secure when you use biometrics to safeguard your financial transactions in concert with other traditional methods such as passwords and PINs.

# CASE STUDY: BIOMETRIC AUTHENTICATION DURING AIR TRAVEL

*Whether you're flying to New York for the weekend or to Paris for two weeks, air travel requires you to verify your identity with government-issued IDs or passports. With the inclusion of biometric authentication at airports, how you verify your identity is changing. Read how biometric authentication plays a role from the moment you check in until you reach your destination and how your privacy is impacted along the way.*

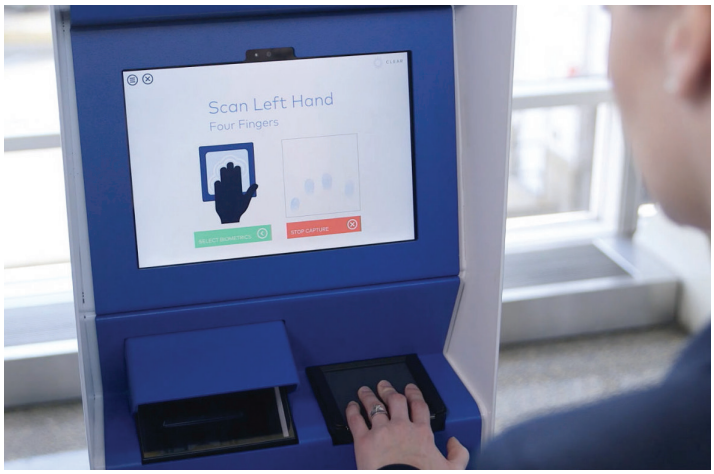
### Check-in and Baggage Drop

You've arrived at the airport with bags for your travel. Checking in usually involves waiting in a long line for an employee to check your ID, verify flight information, weigh your baggage, and hand you the boarding pass. Around the world, hundreds of thousands of people fly every day; biometric authentication allows for quicker travel.

For example, Delta Air Lines has begun testing using fingerprints in place of physical boarding passes. Delta SkyMiles cardholders who fly out of Reagan National Airport in Washington, DC, can use their fingerprint scans to check-in. Delta is also testing facial recognition systems to match your face to your passport photo at Minneapolis-St. Paul Airport to allow baggage check without employee assistance. Initiatives like these can lead to shorter wait times and an increase in traveler numbers.

### Security Check

Moving towards the terminal, TSA checks your boarding pass and ID or passport. Using biometric authentication options at this step gives you access to shorter lines and sends you directly to the scanners. CLEAR is a subscription-based, pre-check program that lets you bypass TSA's ID check after you've set up your biometric profile with a fingerprint and iris scan. When you arrive at a CLEAR kiosk, you scan your fingerprint to authenticate yourself, sending you directly to the physical screening. Replacing a physical ID check with biometric authentication represents the trust placed in biometric data; it cannot be fabricated as easily as traditional identification. CLEAR is available at 24 airports nationwide, so the biometric data is stored digitally to allow multiple access points.




### Arriving At Your Destination

For domestic travelers, there are no additional biometric authentication steps once the plane lands. When you arrive at an international destination, however, customs and border officials often use biometric authentication as an additional security measure, taking your biometric data depending on which country you arrive at. For example, U.S. Customs and Border Patrol collects biometric data from most foreign visitors to verify identity during entrance to and exit from the United States.

Other countries collect even more biometric information at the airport. For example, Singapore's Immigration and Checkpoint Authority use the BioScreen fingerprinting system to collect fingerprints from every foreign visitor for identity authentication upon exit. You scan your passport and then both thumbprints to enter the country. You scan your thumbprint again as you leave to confirm your identity. International travelers are often required to share biometric data with government officials, one of the only times mandatory sharing occurs.

### Conclusion

Protecting your privacy and biometric data during the air travel process means understanding when biometric authentication occurs. Do not participate in any trial-stage biometric programs. Often, a program's full privacy implications cannot be determined during testing. When traveling abroad, determine if you must share your biometric data before you leave. Limiting access to your biometric data keeps such permanent, unchangeable information secure.

*NEXT: PRIVACY: Biometric Data Safeguarding 101*


# PRIVACY: SAFEGUARDING BIOMETRIC DATA 101

***Before you begin associating biometric data with your mobile devices, financial accounts, or travel profiles, you must carefully examine how the company in charge of your account handles this data. Here are some questions to consider before you begin authenticating with your biometrics:***

### Q1. Is your biometric data encrypted?

Biometric data should always be encrypted before storage or transmission. Storing your biometric data as an image (i.e. in the original format as it's captured) can permanently reveal your identity during data breaches. Encryption will store the data as its mathematical representation and add a layer of protection against unwanted exposure.

### Q2. Is your biometric data stored on-device or in the cloud?

Biometric data should be stored only on-device, as this limits data exposure to cases of physical device theft.

### Q3. Can you remotely delete your biometric data?

Privacy-protective policies should have this option in place in case of device loss or physical theft.

### Q4. Can your biometric data be used to match against other biometric databases?

Your biometric data should never be used to match your identity against a database containing biometric information from multiple people (1:N matching) unless required by law. Your biometric data should only be used for verification, also known as 1:1 matching, which only compares your physical features against your own template.

### Q5. Can your biometric data be accessed by the operating system (OS) or any applications running on it?

The OS should only access your biometric data during authentication. 3rd-party apps should never have access to your biometric data.

### Q6. Is your biometric data ever stored on remote servers?

Your biometric data should never be stored in remote servers owned and managed by private companies. They are the most common target of malicious data breaches and attacks.

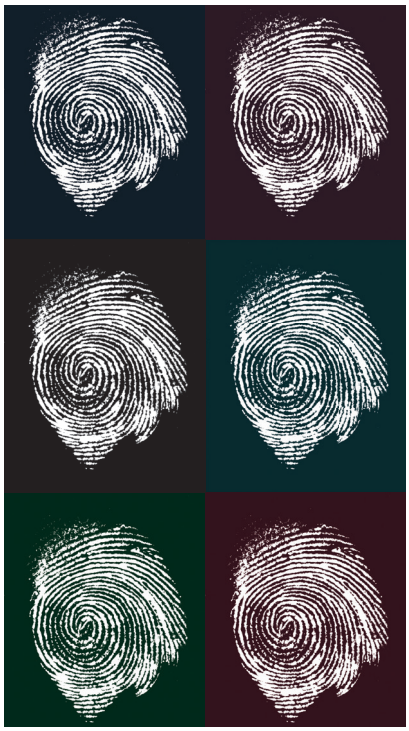
*Sharing your biometric data should be approached with extreme caution as it has the potential to permanently link with your identity. We advise you only do so when companies have established proper protections against all the questions raised in this article.*

# PRIVACY: THE RISKS OF BIOMETRIC AUTHENTICATION

Although biometrics can provide a higher degree of security than traditional passwords, they are still vulnerable to a variety of sophisticated spoofing techniques hackers and other malicious individuals can employ to gain access to biometric-protected devices and accounts.

The theft of more than 21.5 million records from the Office of Personnel Management (OPM) in 2015 gave a foreign entity access to 5.4 million fingerprint records belonging to government employees and contractors. Unlike passwords, which victims can change if they are stolen, victims have no practical way to change their biometrics. These stolen fingerprint records could possibly be used to gain access to devices biometrically-protected devices. Security researchers and consumers are concerned sophisticated groups and individuals may be able to steal biometrics from users and then reuse them to gain access to devices protected by biometric authentication.

In April 2017, researchers from New York University and Michigan State University were able to create a set of "master" synthetic fingerprints by copying and fusing hundreds of real fingerprint patterns. They tested their master prints against many commercially available fingerprint scanners used for authentication and found they were able to fool one scanner 65 percent of the time. Using similar techniques, hackers may be able to fool face recognition systems that do not employ sophisticated anti-spoofing countermeasures.



However, the sophisticated anti-spoofing measures adopted by biometrics professionals make it difficult for hackers and other malicious individual to steal and re-use the biometrics for illicit authentication. Liveness detection is a technique used to verify whether a user is presenting a real, "living" biometric to verify his or her identity. Modern biometric authentication systems such as the Apple iPhone X include sophisticated liveness detection to deter spoofing.

To mitigate these risks, users should employ sophisticated biometric authentication techniques with built-in anti-spoofing countermeasures such as liveness detection. In addition, consumers should use passwords, biometric authentication, and dual factor authentication to maximize protection.

*NEXT: Futures: Authenticating Your Behavior*


# FUTURES: BEHAVIOR-BASED AUTHENTICATION

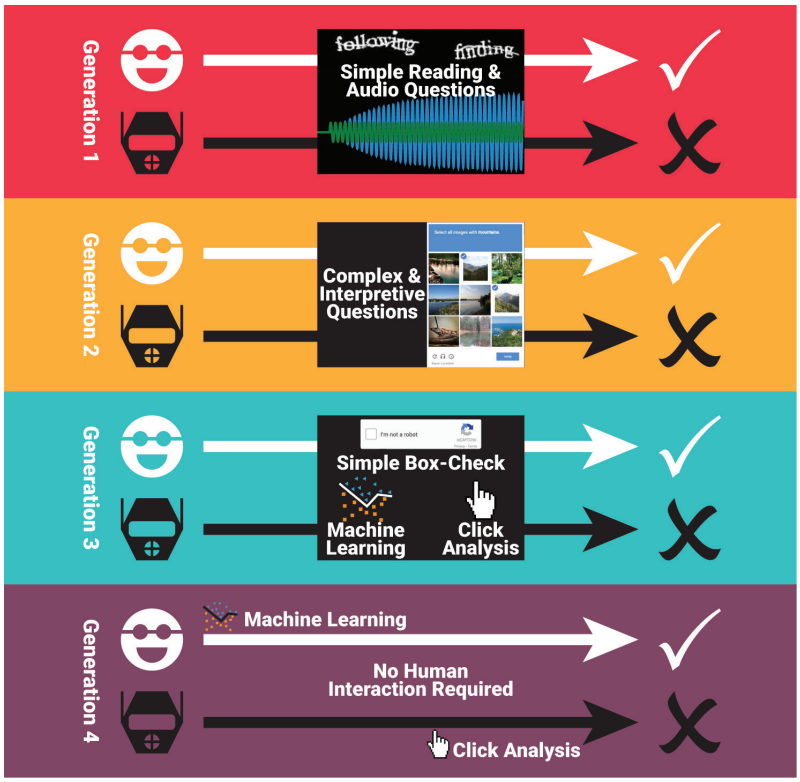
***What if biometric authentication systems, instead of relying on a person's singular and permanent features, looked at a collection of behavioral patterns, in which any single data point alone cannot immediately reveal the person's identity?***

Traditional biometric systems offer security at the point of login by looking at specific physical features. Features such as fingerprint and face are categorized as static biometrics—bodily characteristics that permanently link to the user's identity, and which change minimally over time. Critics often point to the impossibility of decoupling these features with their identity in cyberattacks or data breaches as the main flaw in using biometrics technology in consumer applications. But what if biometric authentication systems, instead of relying on a person's singular and permanent features, looked at a collection of behavioral patterns, in which any single data point alone cannot immediately reveal the person's identity?

Companies are investing in behavioral biometric systems to make this a reality. As the name suggests, behavioral biometrics identify individuals based on the unique way users interact with computer devices and associated hardware, such as smartphones, tablets, or mouse-screen-and-keyboard. By measuring everything from how the user holds a phone or swipes the screen to which keyboard or gestural shortcuts they use, software algorithms build a unique user profile which can then be used to confirm the user's identity on subsequent interactions.

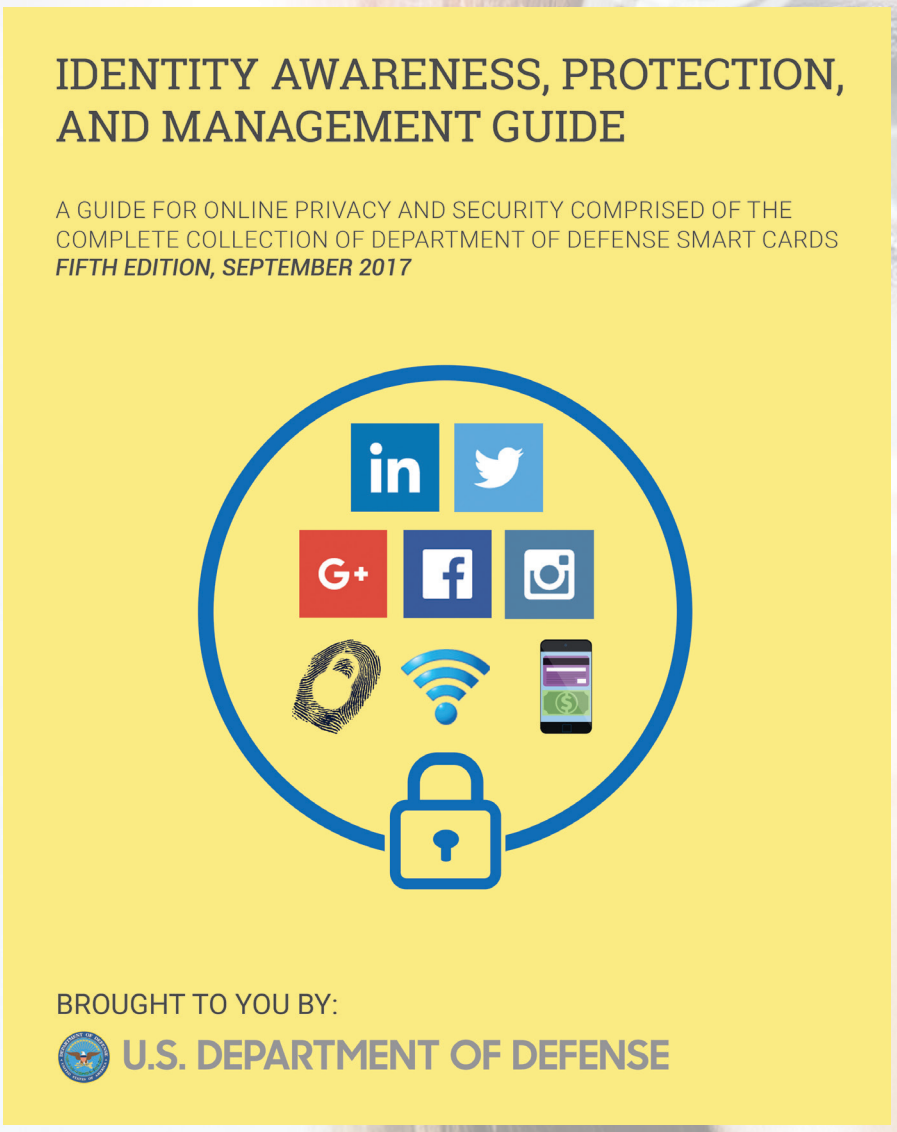
Advocates of behavioral biometrics claim that identification is more accurate and precise because there are dozens of data points collected, and any combination of traits can be used to identify a user. BioCatch, for example, creates an authentication score based on 500 points of behavior. Behaviors can include things like keystroke, scrolling, handedness, password storage habits and more. Its partners, which includes the major credit bureau Experian, can set the "alarm" parameters based on the authentication score generated while a user interacts with a device.

An additional benefit is that authentication can occur continuously throughout the entirety of a secured session versus just at the point of login. One application of continuous behavioral analysis is Google's reCAPTCHA, a system designed to establish that a computer user is human versus a bot. CAPTCHAs, through multiple generations, had always required input from users by responding to a text or identifying images that are challenging for machines to interpret. The latest iteration released in 2017, called invisible reCAPTCHA, completely removes user interaction and recognizes that a user is not a bot simply by analyzing browsing behavior. Though Google uses behavioral analysis at this time only to distinguish a living human from a bot, the same technology could be expanded to identify and authenticate specific individuals without a login interface in the near future.




*Each successive generation of Google's CAPTCHA software requires less behavioral data to distinguish a human user from a bot. How long before a tool can determine who a person is by behavior?*

For more detailed information on protecting and managing other key elements of your identity footprint online please check out the Identity Awareness, Protection and Management Guide.




Send an email to this address to get your copy!
OSD.NCR.OSD.MBX.DODSMARTCARDS@MAIL.MIL