# https://www.axios.com/2020/02/18/biometrics-banking-retail-privacy

**Why it matters: These companies are amassing giant databases of our most personal information — including our gait, how we hold our cellphones, our typing patterns — that raise knotty questions about data security and privacy.**

Banks have been quietly rolling out biometrics to identify customers — verifying them by their fingerprint, voice or eye scan — and retailers like Amazon are getting into the game.

Driving the news: Amazon wants consumers to be able to pay for items in physical stores by waving their palm in front of a payment terminal, the WSJ reports.

The system would link your palm image to a payment card.

Amazon "plans to pitch the terminals to coffee shops, fast-food restaurants and other merchants that do lots of repeat business with their customers," the Journal reports.

Palm biometrics haven't been used for payments on a big scale, but fingerprints have: Apple Pay and the Apple credit card involve pay-by-touch with a cellphone.

**But banks — and, increasingly, retailers — have been working in overdrive to use biometrics both in back-end systems (where consumers won't see them) and public-facing ones:  
  
Chase, Bank of America, Citi and Wells Fargo have introduced various biometric ID options, including voice, fingerprint, eye or facial recognition.**

Palm biometrics haven't been used for payments on a big scale, but fingerprints have: Apple Pay and the Apple credit card involve pay-by-touch with a cellphone.

Voice ID is also prevalent, particularly in bank call centers.

The intrigue: Banks have have had a love/hate relationship with biometrics for decades — customers are leery, and there's a high rate of failure.

As anyone with an iPhone knows, a wet or greasy finger often won't work, and voice recognition systems often fail if someone has a cold (or is tipsy).

Mastercard and Visa are rolling out payment cards with embedded fingerprint ID.  
  
BMO and Mastercard pioneered "selfie pay," which lets customers authenticate themselves for online shopping.

Banks say their systems are completely secure, but they are proceeding gingerly to avoid making their customers nervous.

Several banks gave "no comments" to Axios when asked about their biometrics programs; Amazon did too.

Some banks have dropped the creepier biometrics: Republic Bank of Kentucky said in 2016 that it would let customers log in to their mobile banking app by fingerprint or eye vein scan — now it offers the finger option plus facial ID.

**What they're saying: "A biometric is a very sensitive piece of personal information.**

Some banks have dropped the creepier biometrics: Republic Bank of Kentucky said in 2016 that it would let customers log in to their mobile banking app by fingerprint or eye vein scan — now it offers the finger option plus facial ID.

There are already some horror stories:  
  
Thumbprints have been spoofed with the type of gelatin used in Gummi Bears and a picture of someone else's thumb.

A pair of twins hacked HSBC's phone banking voice ID system — though it wasn't easy.

Facial recognition systems can be foiled by deepfakes, masks, and virtual reality — and they often show racial bias.

If your password gets stolen, you create a new password.

If your fingerprints get stolen, you can't create new fingerprints," Stephen Ritter, chief technology officer of Mitek, an identity verification company, tells Axios.

Reality check: Banking and credit card companies say biometrics — which, so far, are usually optional — are invaluable in fighting fraud and that spoofing is rare.

They call the technology proven and safe, and say that many customers — particularly younger ones — welcome it.

**"If it weren't for being able to use your thumbprint on your iPhone, I think biometrics would still be something on the fringe of authenticating," Trace Fooshee of Aite Group, a banking consultancy, tells Axios.**

Biometric systems have ways of checking for "liveness," to guard against robots and AI intruders.

The systems routinely avert criminal behavior.

One example: Discover, the credit card company, "receives so-called voiceprints of callers — not recordings of their voice — and flags known fraudsters," reports the WSJ.

A growing number of people welcome the convenience, thanks to cellphones making finger ID routine.

On the retail side: Amazon isn't the only company dabbling in biometrics.

The New York Mets have kiosks that will let you pay for snacks by fingerprint.

A handful of quick-serve restaurants like Caliburger and Malibu Poke are letting customers order via facial recognition at self-serve kiosks.

Mitek, which sells a face ID verification system, counts Airbnb, Instacart and Poshmark as customers.

**Between the lines: What customers don't see is banks' and retailers' heavy use of "passive" or "behavioral biometrics" to thwart fraud.**

On the retail side: Amazon isn't the only company dabbling in biometrics.

The New York Mets have kiosks that will let you pay for snacks by fingerprint.

A handful of quick-serve restaurants like Caliburger and Malibu Poke are letting customers order via facial recognition at self-serve kiosks.

Mitek, which sells a face ID verification system, counts Airbnb, Instacart and Poshmark as customers.

"On a mobile phone, that could be the angle that you currently are handling the device, whether you are typing in the password with your thumbs," Chris Reid, EVP at Mastercard, tells Axios.

"Those passive biometrics can tell this isn't actually" the real customer.

The bottom line: Whether we like it or not, biometrics are going to be a bigger part of our lives.

# https://www.santander.com/en/stories/biometrics-the-future-of-security-in-digital-banking

**These types of features are called biometric data and they are becoming increasingly important when it comes to security in digital banking.**

Today, it is possible to verify our identity using a selfie, our voice or by placing our finger on the fingerprint reader of our mobile phone.

Using those features that make us unique is a simple, secure way to access online banking services.

Human beings have physical characteristics that make each of us unique and serve to differentiate us.

We are talking of unrepeatable features such as our facial features, fingerprints and voice.

Just as we can identify our family and friends by simply seeing or hearing them, technology has managed to endow devices such as mobile phones, computers, tablets or video door phones with the same ability.

This protects private data and physical and virtual facilities from access by third parties.

As we have said, biometrics uses those unique, non-transferable features of the human being, so the authentication of security systems consists in creating and saving a model or data map that represents the user exclusively and serves to confirm their identity when they request access, whether to physical or virtual spaces.

Since antiquity, security has been one of society’s major concerns.

# https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-in-banking-is-not-secure

**An estimated 17.6 million Americans were subject to identity theft in 2014, mostly through breached bank accounts and credit cards.**

Yana Welinder is a program manager at Carbon, a non-residential fellow at the Stanford Center for Internet and Society and an affiliate at the Berkman Center for Internet and Society at Harvard.

She is on Twitter (@yanatweets).

This opinion does not reflect the views of the author’s employer or affiliated organizations.

Hacking of banks and identities is big business.

At this point, bank hackers are probably not looking for biometric data when attacking a bank.

But even if it leaks as a by-product of a financial breach, criminals will find ways to abuse biometric data or resell it for further exploitation.

And biometric data is more sensitive than other personal information banks store on behalf of their customers because unlike a credit card number (or even a name!), stolen biometric data cannot be replaced: It corresponds to a person's face or fingerprints.  
  
Being particularly susceptible to attacks, banks should think twice about generating a honeypot of such personal data.

In general, financial institutions tend to invest more in security when they are mandated to do so and, even then, their efforts are mostly focused on minimizing their own financial loss.

**If the compromised data happens to be biometrics, issues of identity theft may simply be unresolvable.**

And biometric data is more sensitive than other personal information banks store on behalf of their customers because unlike a credit card number (or even a name!), stolen biometric data cannot be replaced: It corresponds to a person's face or fingerprints.  
  
Being particularly susceptible to attacks, banks should think twice about generating a honeypot of such personal data.

In general, financial institutions tend to invest more in security when they are mandated to do so and, even then, their efforts are mostly focused on minimizing their own financial loss.

For example, when credit card data is stolen, other personal data of the customer can also be compromised, but credit card issuers do not specifically address that.

It can take customers months to resolve various issues that result from identity theft.

So any regulation of banks’ use of biometrics should be designed to impose sufficient financial loss on the banks to incentivize them to design systems that effectively safeguard biometrics.

It is not enough for banks to simply avoid storing images of fingerprints, faces or irises.

The biometric data that they get from processing those geometries (what banks call “templates”) can also be abused if they are accessed in combination with the algorithm used to extract the templates from the original images.

One exception is when banks use the iPhone Touch ID, which stores all fingerprint data locally on the phone in an encrypted format.

**In that case, banks rely on Apple to tell them whether there is a fingerprint match, and do not access any biometric data themselves.**

So any regulation of banks’ use of biometrics should be designed to impose sufficient financial loss on the banks to incentivize them to design systems that effectively safeguard biometrics.

It is not enough for banks to simply avoid storing images of fingerprints, faces or irises.

The biometric data that they get from processing those geometries (what banks call “templates”) can also be abused if they are accessed in combination with the algorithm used to extract the templates from the original images.

One exception is when banks use the iPhone Touch ID, which stores all fingerprint data locally on the phone in an encrypted format.

Ultimately, it is not clear that biometrics in banking will actually provide better protection than passwords.

If the eye’s iris is the biometric scan, for example, someone could display a photo of a customer’s face into the phone camera to gain access.

Banks claim to address this risk with additional layers of protection like requiring customers to move their eyes.

In an age when sophisticated computer generated renderings could be used to simulate eye movement, it is not hard to imagine how this could turn into a cat-and-mouse game with bank hackers.

**Instead of dabbling in biometrics, banks could focus on software and instructions that push customers to more secure password practices.**

In an age when sophisticated computer generated renderings could be used to simulate eye movement, it is not hard to imagine how this could turn into a cat-and-mouse game with bank hackers.

Customers could get better protection with strong, randomly generated passwords that are not reused between different accounts, are frequently updated and are coupled with two-factor authentication.

There are now password manager apps like 1Password that help users generate secure passwords for all their accounts and keep track of them.

Banks actually often undermine secure passwords by using login software that restricts the use of special characters or prompts customers to answer insecure security questions like "What's your mother's maiden name?"

Join Opinion on Facebook and follow updates on twitter.com/roomfordebate.

# https://www.idmission.com/en/blog/5-ways-biometrics-improve-your-banks-bottom-line

**If your bank is looking for ways to protect your bottom line in the face of increasing uncertainty, you should consider biometrics.**

S&P Global Ratings warns that banks in 2021 could face their toughest year since the aftermath of the global financial crisis.

The ratings agency assigns a negative outlook for almost one third of global banks.

“For many banking systems, we do not envisage recovery to pre-Covid-19 levels until 2023 or beyond,” say S&P analysts.

Deploying biometric identity verification across your banking platforms has a significant positive impact on your bottom line.

From reducing costs to increasing sales, biometrics is paving the way for banks to undergo digital transformation.

Biometric identity verification uses behavioral or physical characteristics to identify whether a customer or employee is allowed access to devices, systems, or data.

Biometric identifiers include facial patterns, fingerprints, voice intonation, and typing cadence.

**With biometrics, retail banks keep sensitive data secure by ensuring that only authorized users are permitted to access it.**

Deploying biometric identity verification across your banking platforms has a significant positive impact on your bottom line.

From reducing costs to increasing sales, biometrics is paving the way for banks to undergo digital transformation.

Biometric identity verification uses behavioral or physical characteristics to identify whether a customer or employee is allowed access to devices, systems, or data.

Biometric identifiers include facial patterns, fingerprints, voice intonation, and typing cadence.

Biometric identity verification systems improve security, speed up the verification process and deter cybercriminals.

Here are the top five ways that biometrics improves your bank’s bottom line.  
  
1.

Biometrics Makes Banking Transactions More Secure  
  
Before fraudsters can steal from your bank, they must first steal an identity.

Fraudulent ATM transactions and criminal online banking transactions are only possible when criminals have banking customer credentials in their possession.

**Biometric identity verification makes banking transactions more secure by adding another layer of security.**

Fraudulent ATM transactions and criminal online banking transactions are only possible when criminals have banking customer credentials in their possession.

They typically get these credentials by stealing them, or by buying them from someone who has stolen them.

Today, these credentials are most commonly a banking card number and a PIN or password.

The trouble is, criminals can easily steal these credentials through phishing emails and malware, exposing your bank to theft, fraud and bottom-line losses.

For example, with facial recognition systems, instead of presenting a bank card number and PIN, customers must also present their face to a facial recognition system, typically in the form of a selfie that they take with their smartphone.

Today’s facial recognition engines use artificial intelligence, machine learning and liveness detection (both active and passive detection) to make it next to impossible for fraudsters to fool these systems with stolen identities, since stealing someone’s face is still fairly difficult to do.  
  
2.

Biometrics Enhances the Customer Experience  
  
A growing number of banking customers are avoiding retail bank branches, and their actions have nothing to do with social distancing or lockdowns or COVID-19.

Today’s banking customers, particularly the younger generation, prefer to do their banking online, often on their phones.

**Biometric identity verification eliminates the friction so common with manual identity verification by letting bank customers identity themselves with their faces or their fingerprints.**

Biometrics Enhances the Customer Experience  
  
A growing number of banking customers are avoiding retail bank branches, and their actions have nothing to do with social distancing or lockdowns or COVID-19.

Today’s banking customers, particularly the younger generation, prefer to do their banking online, often on their phones.

Driving to a branch, finding a parking spot, and waiting in line for a teller to become available are foreign concepts to them.

Banking customers are now demanding that their banking experiences be as seamless, quick and painless as the experiences they have with other consumer-grade experiences, such as hailing an Uber ride, ordering curbside pick-up from McDonalds or watching the latest streaming movie on Netflix.

For example, banks are using technology like IDmission’s Biometric Identity Verification to identify customers in a split second, all from the customer’s phone.

The process is frictionless, and Level 2 ISO-compliant.

The process relies on passive liveness detection, which requires no action from the customer, such as blinking, smiling or turning their head.

Passive liveness detection is the key to improving the customer experience.

**Biometrics Increases Security Across All Access Control Points  
  
If your bank has dozens or hundreds of branches, you know the challenge of employee access control.**

The process relies on passive liveness detection, which requires no action from the customer, such as blinking, smiling or turning their head.

Passive liveness detection is the key to improving the customer experience.

It makes the identity verification process convenient, quick and seamless, while maintaining data security and integrity.

In other words, it delivers the customer experience that bank customers are used to (and now expect) in other areas of their life.  
  
3.

Large, multi-branch banks have critical and complex security requirements.

After all, large numbers of employees routinely need to access multiple physical and logical systems.

Your security is compromised anytime an employee loses their keycard, shares their password or gives away their login credentials during a phishing attack.

Biometric identity verification increases security across your entire enterprise and all access control points.

**Bank employees are required to present a keycard (something they have), a PIN (something they know), and a selfie (something they are, the biometric component).**

Your security is compromised anytime an employee loses their keycard, shares their password or gives away their login credentials during a phishing attack.

Biometric identity verification increases security across your entire enterprise and all access control points.

It offers strong security that, along with passwords or key cards, enables a state-of-the-art, multi-factor authentication (MFA) system that is next to impossible to counterfeit or spoof.

IDmission, for example, provides a unique approach to MFA by adding a biometric layer to your current authentication process.

This biometric-enabled MFA ensures that employees have access to only the areas of your enterprise that they are authorized to access.

Better employee access control means fewer cases of identity theft and hacking.

And that translates into fewer losses and a healthier bottom line.  
  
4.

Biometrics Increases Sales  
  
There are essentially two ways to increase sales.

**Biometric identity authentication helps you do both.**

And that translates into fewer losses and a healthier bottom line.  
  
4.

Biometrics Increases Sales  
  
There are essentially two ways to increase sales.

1. Acquire more new customers.

2. Get existing customers to conduct more transactions.

Let’s start with how to increase sales by acquiring more customers.

Last time we checked, almost 40% of potential new banking customers abandon traditional onboarding processes and head to a digital alternative provided by a competitor.

Today’s bank customers want to access their accounts from any device, from any location, and at any time of the day or night.

If your bank doesn’t offer this convenience and speed, your potential customers will go elsewhere.

**Biometrics reduces customer churn.**

Biometrics increases revenue from fees and interest by letting your customers choose their own experience (whether in-branch or virtual).

When you let your customers bank the way that works for them, they do more of their banking with you.

They pay bills, apply for loans, make purchases, send wire transfers, cash checks and plenty more—all enabled by the convenience, speed and security that biometrics provides.

An added bonus of biometrics is that satisfied customers remain customers.

Customers who enjoy the benefits that biometric identity verification offers continue doing their banking with your bank.

The longer they remain with you, the more fee and interest income you generate.

And the higher your lifetime customer value becomes.  
  
5.

Biometrics Reduces Overhead  
  
Biometrics gives your bank the option of reducing your footprint.

**Deploying biometric identity verification gives you options.**

And the higher your lifetime customer value becomes.  
  
5.

Biometrics Reduces Overhead  
  
Biometrics gives your bank the option of reducing your footprint.

By giving your customers a convenient, quick and seamless way to do their banking online, you reduce your reliance on bank branches and all of the overhead that goes with them.

But going branchless is only possible when the alternative you offer your customers equals or rivals the in-branch experience in terms of services offered, speed of service, customer experience—and ease of customer identity verification.

You can let customers open mobile wallets through biometrics while remaining compliant with regulations.

You can partner with small businesses to act as your agents.

You can offer customers the convenience of making payments using QR codes.

All of these options allow you to reduce your number of branches, and to remove that overhead from your balance sheets.

**Reap the Benefits of Biometrics in Your Bank  
  
One thing you can be sure about is that the world won’t look the same after the COVID-19 pandemic has passed.**

You can let customers open mobile wallets through biometrics while remaining compliant with regulations.

You can partner with small businesses to act as your agents.

You can offer customers the convenience of making payments using QR codes.

All of these options allow you to reduce your number of branches, and to remove that overhead from your balance sheets.

Customers are enjoying the convenience of banking from home on any device, day and night, and you can expect that trend to continue.

If your bank wants to stay relevant to tomorrow’s customers—and stay competitive against today’s rivals—you should deploy biometric identity verification across your enterprise.

Biometrics improves your bottom line by making banking transactions more secure, enhancing the customer experience, increasing security across all access control points, increasing sales, and reducing overhead.

# https://id4d.worldbank.org/guide/biometric-data

**Biometric data**

In addition to biographic data, many ID systems collect fingerprints, iris scans, facial images, and/or other biometry to use for biometric recognition—automatic recognition of individuals based on their biological or behavioral characteristics (ISO/IEC 2382-37).

This process involves comparing a template generated from a live biometric sample (e.g., a fingerprint or selfie) to previously stored biometric(s) to determine the probability that they are a match.

Biometric recognition encompasses both biometric identification—the process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual (i.e. 1:n)—and biometric verification—the process of confirming a biometric claim through biometric comparison (i.e. 1:1) (ISO/IEC 2382-37).

These processes can be used to perform two distinct tasks in foundational ID systems:

**To ensure that each person in a database is unique, ID systems can use biometric identification to perform a duplicate biometric enrollment check.**

This process involves comparing a template generated from a live biometric sample (e.g., a fingerprint or selfie) to previously stored biometric(s) to determine the probability that they are a match.

Biometric recognition encompasses both biometric identification—the process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual (i.e. 1:n)—and biometric verification—the process of confirming a biometric claim through biometric comparison (i.e. 1:1) (ISO/IEC 2382-37).

These processes can be used to perform two distinct tasks in foundational ID systems:

Deduplication of identity records.

This involves comparing a template generated from a captured biometric against all or a subset of templates stored in biometric database to detect a duplicate registration (a 1:N search), after which the new template is added to the database.

This process involves automation as well as manual checks to adjudicate matches.

Authentication of individuals.

Some authentication protocols require biometric verification of the user.

**This involves a one-to-one (1:1) comparison of a template generated from a captured biometric against a single stored template (e.g., one stored on an ID card or mobile phone, or in a database).**

This involves comparing a template generated from a captured biometric against all or a subset of templates stored in biometric database to detect a duplicate registration (a 1:N search), after which the new template is added to the database.

This process involves automation as well as manual checks to adjudicate matches.

Authentication of individuals.

Some authentication protocols require biometric verification of the user.

Biometric recognition has rapidly proliferated in modern ID systems in part because it is currently the most accurate and efficient technology available for deduplicating large populations to ensure statistical uniqueness—particularly in countries without existing authoritative sources of identity information—and because it can provide a relatively high level of assurance during authentication.

As such, biometrics can be a key ingredient in ensuring the trustworthiness of ID systems.

At the same time, however, biometrics are not required or appropriate in all contexts.

In particular, the collection and use of biometric data presents some particular data protection and exclusion risks and can significantly add to the cost of the ID system and add operational complexity.

**The choice to use biometrics—as well as the particular type of biometric data collected—should be informed by these risks and costs, as well as the objectives, planned use cases, and other constraints to the ID system identified in the planning phase.**

Biometric recognition has rapidly proliferated in modern ID systems in part because it is currently the most accurate and efficient technology available for deduplicating large populations to ensure statistical uniqueness—particularly in countries without existing authoritative sources of identity information—and because it can provide a relatively high level of assurance during authentication.

As such, biometrics can be a key ingredient in ensuring the trustworthiness of ID systems.

At the same time, however, biometrics are not required or appropriate in all contexts.

In particular, the collection and use of biometric data presents some particular data protection and exclusion risks and can significantly add to the cost of the ID system and add operational complexity.

Additional analysis on biometric modalities and their use for authentication can be found in the ID4D Technology Landscape report.

In addition, a more comprehensive ID4D Guide on Biometrics is forthcoming.

Types of biometrics Countries that plan to use biometric recognition for deduplication and/or authentication can chose from a variety of biometric characteristics (i.e., “modes”).

In general biometrics fall into two major categories: Biological: fingerprints, face, iris, veins, etc.

**This section provides a brief comparison of the primary biological biometrics used in national-scale ID systems for biometric recognition.**

In addition, a more comprehensive ID4D Guide on Biometrics is forthcoming.

Types of biometrics Countries that plan to use biometric recognition for deduplication and/or authentication can chose from a variety of biometric characteristics (i.e., “modes”).

In general biometrics fall into two major categories: Biological: fingerprints, face, iris, veins, etc.

Behavioral: keystroke dynamics, gait, signature, voice, etc.

For a more detailed evaluation some emerging biometric modalities (voice, vascular, DNA, etc.) see the ID4D Technology Landscape report.

Table 28.

Comparison of biometric technologies commonly used in ID systems Finger Iris Face USE Number available 1-10 1-2 1 Ease of capture

Easy to medium Medium to hard Easy Adjudication Medium—requires trained fingerprint examiner Impossible with naked eye Easy—any person can compare two faces Accuracy for deduplication (1:N) assuming quality capture Very high depending on number of fingers used and population size Very high with 2 irises Low to medium, but improving over time COST Capture device cost 1-print (US$5-40), 2-print (US$200-250), 10-print (US$500-750) US$ 500-1000 Varies from cheap webcam-type devices to more expensive smartphones/tablets Computing for duplicate enrollment check Medium to high—more complicated algorithms require high-end computer cluster with large memory Low to medium—iris matching algorithms are the most efficient as templates are stored in binary code Medium to high—more complicated algorithms require high-end computer cluster with large memory INCLUSION Failure to capture (FTC)

**Other groups with difficulties Manual laborers, persons with disabilities, people with cuts on their fingers, people with diabetes May be more invasive than fingerprints, stigma in some cultures; difficult for persons with visual impairments or albinism Not always optimized for recognition of darker skin tones, some algorithms have difficulty for persons with albinism Source: Adapted from the Digital Identity Toolkit and Technology Landscape for Digital Development, and informed by expert consultations.**

Table 28.

Comparison of biometric technologies commonly used in ID systems Finger Iris Face USE Number available 1-10 1-2 1 Ease of capture

Easy to medium Medium to hard Easy Adjudication Medium—requires trained fingerprint examiner Impossible with naked eye Easy—any person can compare two faces Accuracy for deduplication (1:N) assuming quality capture Very high depending on number of fingers used and population size Very high with 2 irises Low to medium, but improving over time COST Capture device cost 1-print (US$5-40), 2-print (US$200-250), 10-print (US$500-750) US$ 500-1000 Varies from cheap webcam-type devices to more expensive smartphones/tablets Computing for duplicate enrollment check Medium to high—more complicated algorithms require high-end computer cluster with large memory Low to medium—iris matching algorithms are the most efficient as templates are stored in binary code Medium to high—more complicated algorithms require high-end computer cluster with large memory INCLUSION Failure to capture (FTC)

<2-5% ~1-2% ~0% Children <6 years: may not be viable >6 years to adult: usable with software that accommodates for aging <1 year: may not be viable 1-5 years: challenging, requires parental assistance All ages with updates needed over time (accuracy improves at older ages because the face stabilizes)

As shown in Table 28, different biometric modes vary in terms of their: Accuracy .

The accuracy with which the technology matches records.

This includes the false match rate (FMR) and false non-match rate (FNMR) of the technology.  
  
Universality .

The presence and ease-of-capture of the biometric in members of the relevant population and in a variety of climates and weather conditions.

**The ease with which individuals can interact with the technology used to capture the biometric data and its utility for different purposes (e.g., some biometric modes may be more convenient for authentication than others)  
  
Cost.**

The permanence of the biometric over time (e.g., for children, or the elderly) or after disease or injury.

Collectability .

The ease with which good quality samples can be acquired.

Usability .

The hardware and software costs of collecting and matching samples during initial registration and—if used for authentication—at points of transaction.

In practice, many countries adopt a multimodal strategy and collect more than one type of biometric data.

This is beneficial for multiple reasons: More accuracy.

More data points (e.g., fingerprints and iris scans or fingerprints and face) help ensure statistical uniqueness to a higher degree of accuracy, which may be necessary in large populations (see Gelb & Clark 2013b)

**More modes can help increase the possibility that all members of the population are able to provide a biometric sample (e.g., fingerprints may be difficult to collect for manual laborers, but iris scans may work).**

In practice, many countries adopt a multimodal strategy and collect more than one type of biometric data.

This is beneficial for multiple reasons: More accuracy.

More data points (e.g., fingerprints and iris scans or fingerprints and face) help ensure statistical uniqueness to a higher degree of accuracy, which may be necessary in large populations (see Gelb & Clark 2013b)

Improved inclusion and fault tolerance.

Allows for the use of different biometrics (fusion) for deduplication and authentication.

Certain biometric modalities may be optimal for conducting duplicate biometric enrollment checks (i.e., 1:N/N:N matching, while others may be optimal or sufficient for use during authentication (1:1 matching).

The choice of which biometrics to use—if any—will have implications in terms of the trustworthiness and inclusivity of the ID system, as well as potential risks.

These issues are discussed below, with particularly attention to inclusion challenges, use with children, and concerns regarding privacy and exclusion.

**Practitioners will also need to make related decisions regarding the technical standards used for biometric recognition, as well as back-end systems used for biometric deduplication.**

Allows for the use of different biometrics (fusion) for deduplication and authentication.

Certain biometric modalities may be optimal for conducting duplicate biometric enrollment checks (i.e., 1:N/N:N matching, while others may be optimal or sufficient for use during authentication (1:1 matching).

The choice of which biometrics to use—if any—will have implications in terms of the trustworthiness and inclusivity of the ID system, as well as potential risks.

These issues are discussed below, with particularly attention to inclusion challenges, use with children, and concerns regarding privacy and exclusion.

Figure 21.

Key considerations for using biometrics Inclusion Reliability Data Protection Sustainability Certain biometrics may be difficult or impossible for some people to reliably provide, necessitating multimodal biometrics and/or appropriate technical and procedural measures to reduce exclusion.

Biometric deduplication may be the best solution to establish uniqueness in large population, however, not all biometric modes provide the same level of accuracy.

The use of biometrics creates additional risks to privacy and data protection that must be mitigated through legal, technical, and operational controls.

**Biometrics can add significant costs to registration as well as the authentication infrastructure.**

Figure 21.

Key considerations for using biometrics Inclusion Reliability Data Protection Sustainability Certain biometrics may be difficult or impossible for some people to reliably provide, necessitating multimodal biometrics and/or appropriate technical and procedural measures to reduce exclusion.

Biometric deduplication may be the best solution to establish uniqueness in large population, however, not all biometric modes provide the same level of accuracy.

The use of biometrics creates additional risks to privacy and data protection that must be mitigated through legal, technical, and operational controls.

Challenges for accuracy and inclusion In deciding the set of biometrics to use, special attention needs to be given to the ability to collect these characteristics from the entire population.

For example, there are specific groups and conditions—both of which may be overrepresented in developing countries—where FTE errors during enrollment and FNMRs during biometric verification are likely to be more common.

Where individuals are unable to enroll, or where authentication procedures fail to confirm that a person is who they claim to be, this will lead to exclusion.

There are three categories of people that present difficulties for biometric recognition, including: People who cannot physically provide an acceptable biometric (e.g., amputees, survivors of leprosy, etc.) to enroll in the first place  
  
People for whom acquiring reliable biometric samples is difficult (e.g., manual laborers, elderly people, children, people with visual impairment, persons with albinism, etc.) which could make enrollment or authentication difficult  
  
People who decline to provide their biometrics (e.g., because of religious or cultural constraints, such as the appropriateness of data capture techniques that require physical contact to get accurate readings)

**Minimal training or low capacity of the operator capturing the biometrics Lack of incentives and/or time for capturing quality data Poorly implemented enrollment and quality assurance process  
  
Biometric system characteristics: Quality of the biometric scanners and software, including the Automated Biometric Identification System (ABIS) and other software development kits that may be used The statistical nature of biometrics Changing properties of biometric characteristics (i.e., facial appearance over time) Non-optimum threshold setting for matching algorithm—i.e., the tradeoff between the FMR and FNMR  
  
Some of these issues may be addressed through: Designing a multi-biometric system (see above) to ensure that most people are able to provide at least one viable sample  
  
Optimizing enrollment procedures, including by using: Better capture devices and software with built-in quality assessment to improve data quality and reduce FTE Quality Assurance Process and standards (e.g. NFIQ-II) Conditioning materials (gels, alcohols, etc.) that improve finger image contrast Uniform background for facial images Choice of capture devices (small versus large scanners, 4-4-2 versus single fingerprint scanners, optical versus capacitive)**

For example, there are specific groups and conditions—both of which may be overrepresented in developing countries—where FTE errors during enrollment and FNMRs during biometric verification are likely to be more common.

Where individuals are unable to enroll, or where authentication procedures fail to confirm that a person is who they claim to be, this will lead to exclusion.

There are three categories of people that present difficulties for biometric recognition, including: People who cannot physically provide an acceptable biometric (e.g., amputees, survivors of leprosy, etc.) to enroll in the first place  
  
People for whom acquiring reliable biometric samples is difficult (e.g., manual laborers, elderly people, children, people with visual impairment, persons with albinism, etc.) which could make enrollment or authentication difficult  
  
People who decline to provide their biometrics (e.g., because of religious or cultural constraints, such as the appropriateness of data capture techniques that require physical contact to get accurate readings)

In addition, there are other factors that can lead to accuracy and inclusion challenges with biometric recognition, including: Environmental and procedural issues: Harsh conditions, such as direct sunlight, excessive wind, dust, humidity, and dryness, etc.

Implementing comprehensive training of operators to ensure understanding of and adherence to protocols To ensure the inclusion of this group, it is vital that the identity provider develop transparent and practical methods of exception handling.

For duplicate biometric enrollment checks during registration, this could involve identity proofing by other means, such as witnesses, alternate documents, demographic deduplication, and more.

For authentication, there must be alternative methods of proving someone’s identity when biometric verification fails or is not possible, in order to ensure that people are not denied access to rights and services for which they are eligible and entitled.

Exception handling procedures must be complemented by strong grievance redressal mechanisms to ensure that no one is excluded or unfairly treated as a result of the ID system.

**This is also true for any other type of authentication method and is not limited to the use of biometrics.**

Implementing comprehensive training of operators to ensure understanding of and adherence to protocols To ensure the inclusion of this group, it is vital that the identity provider develop transparent and practical methods of exception handling.

For duplicate biometric enrollment checks during registration, this could involve identity proofing by other means, such as witnesses, alternate documents, demographic deduplication, and more.

For authentication, there must be alternative methods of proving someone’s identity when biometric verification fails or is not possible, in order to ensure that people are not denied access to rights and services for which they are eligible and entitled.

Exception handling procedures must be complemented by strong grievance redressal mechanisms to ensure that no one is excluded or unfairly treated as a result of the ID system.

Children and biometrics One persistent inclusion challenge with ID systems that use biometrics is that many biometrics take time to develop or stabilize after birth.

For example, the viability of the following modes depends on age (see also Table 28): Fingerprints (6+ with update).

The papillary ridge structure does not develop before the age of six, which means that reliable fingerprint minutiae—the points of comparison in a biometric template—are difficult to extract before that age.

Furthermore, aversion to the capture process (i.e., squirming) makes it difficult to collect quality samples.

**Given that it is currently not feasible to capture stable biological biometrics at birth—nor are there yet clear use cases as part of a foundational ID system—countries have a few options for the use of biometrics for children in an ID system.**

Iris (~1-2+).

The iris is fully formed 1-2 years after birth but poses some difficultly in capture and requires significant assistance from the parents until around five years of age.

Photos (0+ with updating).

Images of the face can be captured from birth, but they need to be updated frequently in the first years of life in order to be useful for automated recognition.

The first option is to enroll young children without biometric information—or with information that will change over time—and either add or update this information at a later date (e.g., at the first year of high school, for practical reasons).

A second option is simply to only include older children and adults in the ID system.

Typically, such solutions also include linking the child’s record with their parents (see Box 29), which can also help establish statistical uniqueness of a child at the point of birth registration.

Box 29.

**The biometric data for the child must be uploaded when they turn five years old, and the identity re-registered at age 15.**

A second option is simply to only include older children and adults in the ID system.

Typically, such solutions also include linking the child’s record with their parents (see Box 29), which can also help establish statistical uniqueness of a child at the point of birth registration.

Box 29.

Examples of incorporating children into an ID system with biometrics or alternative methods of establishing uniqueness In the Indian state of Haryana, children are enrolled in Aadhaar using a parent’s number which is biometrically authenticated.

Peru’s ID system also collects infant biometric information (such as footprints and a photo) in combination with parent’s fingerprints.

Countries may also implement a mandatory renewal period in order to update children’s biometrics and other information.

In Argentina, for example, children are required to renew their ID at age 8.

Indonesia’s population register (SIAK) covers all ages, however biometrics are collected at age 17 (or younger for married women) for the issuance of a national ID smartcard (e-KTP).