The Top 8 Myths About Biometric Authentication Technology

Biometric authentication technology can secure access to what's important to us online...

such as our data, finances, and key digital services. It can afford us effortless access while keeping fraudsters out. And it can do this in a way that's far more secure, inclusive, and convenient than traditional methods (such as passwords).

But the truth is that many people have reservations about biometrics. Some of these are well-founded, and some aren't. New technology such as airplanes, telephones, and television were all considered groundbreaking at one point too, and people can tend to fear what's not fully understood. Plus facial biometric verification technology is often confused with facial recognition for surveillance — but more on that later...

Before you read on, keep in mind that not all biometric authentication technologies are created equal, so it's vital to pick the right biometric authentication vendor. In this document, we're primarily talking about **iProov facial biometric assurance technology**. Other vendors' solutions cannot make the same claims about inclusivity, convenience, security, privacy, and so on.

So, let's go ahead and dispel eight of the most popular myths about biometrics!

Myth: Biometrics Can Be Stolen

Biometrics can absolutely be copied. There's nothing secret about your face — millions of us post photos on social media all the time. But while your possessions (like a mobile phone) or secrets (your password) can be stolen, biometrics can only be forged. You can't steal someone's face.

You can get hold of a photo or a video, or make a mask that looks like someone else, but these are copies — and if the authentication technology can verify your genuine presence, the thief won't succeed with a photo or a mask. Most biometric authentication technologies will implement anti-spoofing tactics to distinguish between falsified and authentic users. These methods might include:

- Using advanced machine learning to identify the subtle cues and micro-movements that the human eye is unable to detect.
- Analyzing the interaction of light on skin as in the case of iProov's patented Flashmark technology.
- Requiring the user to follow instructions, such as smiling or turning their head (though many providers have moved away from active to passive biometric solutions in order to maximize convenience and inclusivity).

Ultimately, biometrics aim to prove that you are who you say you are. And unlike possessions and passwords, who you are cannot be stolen.

Myth: Biometric authentication is the same as face recognition

The use of face recognition for surveillance is completely different from authentication. Biometric authentication:

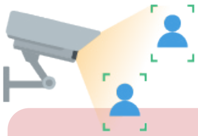
- **Requires collaboration from the user**
- **Provides a direct benefit to the user**
- **Makes the user aware that it is happening**

Face recognition for surveillance, on the other hand, is usually done without the knowledge or collaboration of the individual.

Face Verification

Face verification is a process where the user:

- **KNOWS** the process is happening
- **COLLABORATES** with the process
- **BENEFITS** from the process
- Is assured of **PRIVACY** protection



Face Recognition

Face recognition is a process wherethe user:

- **DOES NOT KNOW** the process is happening
- **DOES NOT COLLABORATE** with the process
- **DOES NOT DIRECTLY BENEFIT** from the process
- Has no control of **PRIVACY**

3

Myth: Biometric authentication infringes on your privacy

The storage of biometric information has more stringent controls than the storing of information posted to social media sites or shared with ancestry research firms via DNA testing.

iProov's biometric authentication systems have privacy built in by design. As far as iProov is concerned, all users are anonymous due to the use of a privacy firewall. To safeguard the user's confidentiality, strong encryption techniques protect all user data, such as face biometrics. Data is never shared with any third party.

The principle of the privacy firewall is to ensure that iProov's biometric authentication system remains ignorant of who the user is. The firewall strips away any PII that might identify the user. Instead, each user is identified to iProov by a meaningless serial number. So while a bank, government, or other iProov customer knows who their user is, iProov never receives that information. The data iProov receives is useless for any other purpose — commercially or to a criminal. In Europe, this approach to privacy protection is known as data minimization and pseudonymization, and both are recognized as powerful ways to protect the privacy of citizens. Privacy-sensitive organizations around the world who rely on iProov agree.

It's also important to note that the processing and storage of biometrics for authentication is governed by GDPR for EU vendors and other stringent regulations across the world.

4

Myth: Biometric authentication is intrusive

Badly designed biometric authentication can yield an unpleasant and intrusive user experience. But if the system has been designed to put the user at the heart of the experience, it will not be invasive.

The process of scanning a face should require nothing more than a simple positioning of the face and a scan lasting a few seconds — there should be no complex instructions.

iProov's biometric solution is convenient and doesn't require the user to do anything: it's passive. The user is aware that it is happening, and they get direct benefit (such as access to their account or effortless onboarding).

Myth: Biometric authentication is too high-tech or expensive

Adjusting to new technology takes time. The advent of face biometrics on mobile phones has changed people's perceptions of it. Prior to 2017, face biometrics were considered to be futuristic and exotic. Now, virtually everyone has understood that it can make life easier.

Thanks to Face ID, Touch ID, and other face or fingerprint verification tools, users are familiar with using biometrics to authenticate themselves. iProov research conducted in March 2021 showed that 70 percent of Americans who use mobile banking either already use face verification to access their accounts or would do so if their device supported it.

The truth is that traditional authentication is no longer fit for purpose. The cost of resetting and maintaining other authentication methods, such as passwords, is growing. Gartner found that 20-50% of all service desk calls were for password resets, and Forrester research cited several organizations that allocate over $1 million per year for password-related support costs.

On the other hand, biometrics can usually be deployed extremely quickly and at a huge scale. You can't "forget" or lose your biometric. And if, like iProov, the provider is cloud-based, there's no need for any identity recovery because the credentials are stored in the cloud rather than a device. This makes authentication device-agnostic. Ultimately, biometrics can be an efficient solution and a time/cost-saving initiative.

6

Myth: Biometrics are vulnerable to data breaches

Many people have an (incorrect) notion that biometric data is stored in one large database as raw images, which are accompanied by each person's full name and personal information. Certainly, this could be true for badly designed biometric systems — as with any security system. But any company worth engaging with will encrypt all of its biometric data and associate it with an anonymous pseudonym.

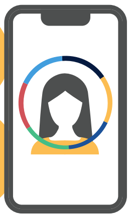
For instance, even if a hacker managed to access iProov's cloud servers, instead of imagery they would find an anonymized binary code. This is called a biometric template, which is entirely useless to an attacker. The template functions as a unique representation of the person, but it is not an image.

7 **Myth:** Biometric authentication is unreliable

Biometric authentication is now extremely accurate and reliable. While a poorly constructed biometric system could deliver poor results, a well-designed system that prioritizes user experience as well as security will deliver unrivaled accuracy and high success rates.

Comparatively, credential or knowledge-based authentication methods present far more problems. 80% of hacking-related breaches still involve compromised and weak credentials — i.e. stolen passwords. This is largely because people share, write down, forget, and reuse their passwords. An iProov survey found that 34% of 18-24s are having to request a reminder for forgotten passwords at least once a week. These factors all combine to make passwords a far more “unreliable” and vulnerable option than many biometric authentication technologies.

8 **Myth:** Biometrics are impersonal or unnecessary



In the past decade, it’s become accepted that we must be able to verify and authenticate people remotely. It’s also become clear that information and facts about a person – such as a password or secret answer – are not enough to truly trust someone online.

Some countries prefer using methods such as video conferencing for online verification. But with the progression of deepfake technology, it can be difficult to trust the genuine presence of a person this way. Additionally because this method is manual, it’s slow, inconvenient, difficult to scale, expensive, and can be less accurate.

Biometrics can be convenient, scalable, and quick – how long does it take you to stare into your phone’s user-facing camera? Now compare this to the time it takes to reset a password or copy an SMS code from your phone when authenticating on a computer…

Biometric authentication can make the internet a much safer place, while also making onboarding and authentication easier and faster. Biometrics can establish trust online in a way that’s secure, inclusive, and convenient. That’s why they’re necessary and why we need to overcome the myths to provide reassurance.

If you’d like to learn more about biometric authentication, you’re in luck: we’ve written the complete guide! Download your free copy of Biometric Authentication For Dummies here. And if you’d like to learn more about how iProov can secure and streamline your organization’s online verification, authentication, and onboarding, book your demo today.