IDEMIA

IDEMIA's Top 4 Trends in Biometrics for 2020

As the world leader in biometric solutions, IDEMIA explores the top four biometric trends for 2020.

JUSTICE & PUBLIC SAFETY

POSTED ON 01.28.20

The full potential of biometrics is yet to unfold. The public and private sectors drive its growing usage. In our increasingly connected world, biometrics is set as one of the key enablers of its digital transformation. Today, the biometric industry's central focus is to protect our identity and improve security for all of us.

1) Use of multi-biometric identification adds a further level of security

As the only form of **biometrics** that leaves a visible trace, our **fingerprints** were the first biometrics widely used for identity verification. Today, other biometrics such as face, iris, and DNA are commonly used as well. 2020 will see more and more solutions that offer **multi-biometric identification**. The combination of multiple types of biometrics enhances security and adds granularity. Depending on the nature of transaction or interaction, different levels of **security** might be needed. We can already unlock our smartphone with either our fingerprint or face, as this is a comparably less sensitive action. In contrast, mobile biometric devices using fingerprints and faces have, for example, been developed for law enforcement agencies, enabling officers to verify the identities of individuals while patrolling the streets. Another example is the national eID card in Nepal. Nepalese citizens can use their ID cards to interact with their bank, which is why both fingerprint and iris data are embedded into the card for maximum security. 2020 will see this trend growing.

2) Increased exposure of biometrics calls for top-notch technology to secure data

Today, public and private sectors alike face the challenge of achieving two aims simultaneously:

1. Enhanced, convenient services in a digital world
2. Prevention of identity theft when using these services

Biometrics is the safest way to verify one's identity. With the assistance of advanced technologies, the verification of identities with biometrics is fast and easy. However, due to their increased usage, **biometric data** becomes ever more exposed.

On top of this, the trend of storing data in the cloud increasingly includes even the most sensitive data. From startups to large multinationals, cloud computing has revolutionized the way many organizations store and interact with data. It facilitates easier data management, flow and sharing.
Biometric data is arguably one of the most sensitive types of data that one can get hold of. 2020 will be all about developing ways to provide extremely tight cyber security to protect biometric data – in the cloud or wherever it might be stored, processed or shared.
Three ways of securing data will ensure we can continue to benefit from convenient services and security at the same time, and feel confident in sharing our data:

1. **Secure multi-party computation**. While securing data in rest and in transit is quite common, the trickiest part is to secure data that is being processed. Traditionally, the processing party had to be able to 'see' data to be able to work with it. The risk connected with this method is significantly reduced when the work of processing the data is shared between different parties. It means that there is not one central player processing all the open, vulnerable data, but several contributors. Only by breaching the data processed by each player would the data make sense to the malicious perpetrator. In 2020, we will see a much wider application of this methodology.
2. **Verifiable computing**. For the security of biometric data, this is a very interesting trend in data processing, which will further develop in 2020. Verifiable computing means that one central entity can outsource the computing of data to another potentially unknown, not previously verified entity, while maintaining verifiable results. In the world of biometrics this could mean that we could do the matching of our own data to verify our identity, for example on our smartphone (i.e. the unknown, not verified entity), without anyone doubting the validity of the computing we have done. This would mean that we control our biometric data at all times and it would never leave our own device.
3. **Homomorphic encryption**. Homomorphic encryption already protects data both at rest and in transit. However, the Holy Grail that we will see developing in 2020 is to apply this encryption technology also to data that is being processed. The goal is simple – to ensure the data processor cannot decipher or even understand the content that is being processed. It is a method of performing calculations on encrypted information, without decrypting it first. In 2020, we will see a movement towards standardizing homomorphic encryption on a worldwide level. The standard will give a boost towards the aim of using encrypted biometric data while computing. With this last step, end-to-end data privacy can be achieved, given that at no moment in time data is exposed without protection.

3) Wide-spread adoption of facial recognition technology

With high performance levels in terms of speed and accuracy, it is no wonder that we will see a wide adoption of **facial recognition** technology in 2020. Already over the last few years, many use cases have demonstrated how this technology brings convenience and security. It is one of the least intrusive biometric identification methods because it requires little behavioral adaptation.
Today, **facial recognition** is already used to enable security and convenience. It is, for example, an important facilitator to manage the increasing number of travelers globally. In Europe, over 18 countries are using facial recognition, allowing 200 million passengers to cross borders using their face[1]. Banks have also started to deploy biometric-based systems, so users no longer need to visit branch offices when opening new bank accounts. They simply capture a picture of their ID and take a selfie. **Liveness check functionalities** permit the customer to prove who they are with a few movements of their head, ensuring a photo or video of them is not used to impersonate them[2].
As facial recognition continues to be widely implemented, what are some of the new use cases we should expect to see in 2020?

1. **Protection of public places with video analytics.**
   Enhanced video analytics add intelligence to existing video surveillance. This technology will in 2020 play

- an increasingly important role in providing effective solutions to detect threats. Combined with efficient incident response platforms, **video analytics** enable the law enforcement community to react quickly when a person of interest is detected in a vulnerable area. The analytics provided can be compliant with the strictest data protection laws; detecting **biometrics**, i.e. face, is by far not their only capability. Next year, we expect to see this type of tool widely offered and therefore a sharp increase in its use.

2. **Facial recognition in new industries**.
   While most use cases for **facial recognition** involve the public sector, many technically advanced industries are expected to implement facial recognition technology for security and convenience as well – like the automotive industry. In 2020, more and more proofs of concept will emerge enabling drivers to access their vehicles and start the engine by simply showing their face. Thanks to facial recognition, the vehicle will automatically adjust the temperature settings, move the seat precisely to fit physical characteristics and preferences and load personalized data, including music playlists and navigation settings into the infotainment system. Moreover, facial recognition replaces the need to look for physical keys (or mobile devices) to open a vehicle and drive away. This improves security by defeating "relay attacks", where the signal from a car key is captured by the perpetrator within the vicinity of the car using a special device, and car hijacking attempts as the car can only be driven by recognized drivers.

4) Development of a regulatory and ethical framework for the use of facial recognition

Facial recognition technology offers significant problem-solving potential for both security- and convenience-related use cases. Yet as its use is based on monitoring people's movements, this specific type of biometric data is particularly personal. Citizens have to keep control of their **biometric data**. They need to know how their data is used, how long it is saved and for what reason. To address unease, 2019 has already seen several attempts to develop regulatory and, arguably more importantly, ethical frameworks that define the way facial recognition technology should be used. IDEMIA expects this trend to grow in 2020, with national initiatives being escalated to a continental or even global level. As a leading provider in the industry, IDEMIA encourages the cooperation between governments, the private sector and providers of the technology to define a framework that allows all stakeholders and end-users to benefit from this technology while addressing the public's concerns.

---

[1] Secure Identity Alliance 2019: Biometrics in identity: Building inclusive futures and protecting civil liberties
[2] https://www.intelligentcio.com/me/2019/07/29/bank-abc-employs-biometrics-from-jumio-to-streamline-digital-onboarding/
