POLICY BRIEF

9 / 2021 — Digital

The body as an access key? Biometric methods for consumers

Key points

Mobile phones are trailblazers for biometrics, which is creeping its way into our daily lives. Many find it is a harmless and safe norm to identify yourself or pay using your fingerprint, just to name two examples how biometric methods find their way into consumers‘ everyday life.
However, there is a downside to this trend:

- **Flawed**

A person cannot be identified as clearly as applications often claim - tests using dummies show how easily a system can be outsmarted. Furthermore, the Vienna Chamber of Labour is aware of cases where the safety bar has been circumvented within a family: a father and a child - although far apart in age - are able to unblock the father’s mobile phone due to the similarity of their features.

- **Open to abuse**

If a fingerprint or facial scan falls into the wrong hands, the damage caused by identity theft cannot be remedied. Unlike passwords, fingerprints cannot be changed. In addition, we are talking of highly sensitive data that can reveal much about the health, origin, etc. of a person.

- **Irreparable damage**

You cannot delete biometric features. They accompany us until we die. Lost keys and forgotten passwords can be replaced, but your physical characteristics cannot. If prints, scans, etc. were stolen for illegal purposes, this would have permanent consequences. In case of a PIN it’s easy to protect, you simply do not reveal it to anyone. However, we leave our fingerprints everywhere, every day.

Background

Biometrics can be useful as an additional safety component for identification and authentication processes. However, the use of biometrics is only sensible in exceptional cases, where the risk of data misuse is very low, the data life cycle is very short, data are not processed or stored centrally, and biometric data cannot be copied technically. Using biometrics as a key does not enhance security in any way. Therefore biometric data are more appropriate to unequivocally identify a person when they are physically present. An example of that are photographs and other biometric features in passports.

Standard procedures with the use of password also function when the consumer is not present. It is therefore assumed, erroneously, that biometrics increases security. However, there are endless risks of misuse: for example, a fingerprint can be lifted using adhesive tape or, even simpler, using the photograph of a fingerprint from glass, as safety researchers have demonstrated. This can be used to create a print that allows unauthorised access without the need for the original fingerprint. Even standard digital cameras are capable of outwitting fairly complex biometric procedures such as iris scans. Facial recognition is extremely vulnerable because images of faces can be found in their millions on the Internet and they are unprotected. This means that people’s biometric data can be generated remotely and misused. For example, unblocking a smartphone and activating the login via facial recognition can easily be circumvented using the photograph of a person’s face. Other means are copying unique hash values for biometric characteristics, for example by hacking into biometric databases to steal the corresponding information. Such cases have been on the rise in recent years, as various hacks of large biometric databases in the public and private domain show.

Main findings

A recent study by the Institute for Technology Assessment (Institut für Technikfolgen-Abschätzung) looks at the impact of the wide-scale use of biometric procedures on consumers and society as a whole and comes to the conclusion:

Data transfer defies any control

In the case of biometric characteristics recorded by sensors, such as image or acoustic data, it is not possible to track whether the data of those concerned have been passed on or not. Above all, systems in standby mode, e.g. virtual assistants or motion activated cameras, have already fallen into disrepute in this regard. We are unintentionally constantly leaving behind our fingerprints or traces of our DNA. However, also the imprudent publication of picture or sound recordings can result in biometric characteristics being passed on unwittingly. It was possible to create replicas of important iris or fingerprint characteristics of German politicians using high-resolution press photos.

Hidden or subsequent data analysis

A peculiarity of biometric characteristics is that they can often be used for identification without the knowledge or conscious support of the person concerned. The recording of biometric characteristics often appears to simply be the side effect of its actual function. The use of iris cameras, voice recordings from a microphone, or the analysis of internet profile images is either concealed from the customers or done initially for a completely different purpose. Data can be recorded very easily without the person's knowledge and it is even easier to analyze the data in the following biometrically. Experts doubt whether biometric data (such as facial images) on smartphones are sufficiently protected against further use by third parties. Third parties can, for example, have access to facial scanners, as it is known in the case of iPhones.

Voice recordings or facial images can be exploited long after the data were actually recorded, as scandals such as Clearview or PimEyes show, where large sets of data containing facial images were used subsequently on social networks or online, and the biometric characteristics of which were exploited.

Enormous legal gaps related to biometric data

Biometric data are most certainly sensitive data and hence require particular protection. The GDPR contains a legal definition of the term "biometric data"; however, it is not sufficient to protect only these "biometric data in the narrower sense". There are endless amounts of biometric data not covered by this legal definition (e.g. facial images on the Internet) - so-called "biometric data in the wider sense". Since they are widespread and are subject to the same possibilities of exploitation, the protection of the GDPR should have been expanded long ago.

Trend toward simple "convenience" for consumers

The spread of biometrics in everyday technical systems and commercial applications (finance and banking sector) should not be viewed with complacency when you consider that it was once a surveillance technology intended for military and security purposes. It is often used as an additional factor in banking apps and e-commerce according to the EU Payment Services Directive. However, the overall gains in security are often only marginal or counter-effects can even be observed. The associated familiarity lowers the inhibition threshold among users, often also at the same time their concerns about security, and their awareness of possible risks. The main risks include, apart from a greater risk of the misuse of biometric data, a creeping compulsion to identify yourself in many areas, mass surveillance using biometrics, and finally a possible end to anonymity.

Facial recognition as a particularly worrying application

Facial recognition plays a special role in this development. Although systems still show high error ratios and people are therefore repeatedly categorised as suspects, they continue to be used by security agencies. In addition, the algorithms used have a bias that can give rise to racism and discrimination. On the whole facial recognition is used for mass surveillance; this is considerably more noticeable in the US, but even in Europe it is becoming more prevalent. Its growing ubiquity means that this technology poses a major danger to democracy.

The trick with dummies

Studies on artificially generated, statistically optimised fingerprints show how easy criminal attacks are. These fingerprints would adequately match numerous biometric models of actual fingerprints and hence create a type of master key for a biometric system. Several facial images have also been successfully merged into one synthetic facial image, whereby several real faces were assessed as matching the biometric facial models. The manufacturers of access systems are trying to combat this by collecting even more data, e.g. skin resistance or 3D facial forms for liveness detection.

Empty security promises

Not even digital facial templates can offer total protection against data misuse. In the relevant literature the possibility was discussed, for example, of recreating biological characteristics based on templates. The storage location could help to ensure data security. If biometric characteristics are exclusively stored on the local end device of the consumer, subsequent data misuse through copying by a central body becomes at least less probable. However, offerors derive more benefit from centrally held data sets (e.g. algorithmic improvements to their services).

Illegal commingling of authentication and identification

Authentication is proof of a certain characteristic and it does not necessarily require the identity of a person to be ascertained. This means that no identity data need to be processed for authentication purposes. Where biometrics are used, this is inevitably linked to the identity of a person and it is scarcely possible to separate the two. A simple example is eligibility, based on age, to watch an age-rated film. It is sufficient to know the age of a person. A simple digital process compares the date of birth with the current date in order to ascertain a person's age and hence whether they are entitled to watch the film. If biometric data are being used, identifiability inherent in biometric data is provided as an added bonus. The important, clear separation between authentication and identification in the sense of data protection and security is significantly more complicated when biometrics are involved.

The pandemic as an additional driving factor for collecting biometric data

The Covid-19 pandemic has shown how quickly the collection of biometric data can spread. Some countries are making increased use of biometric systems in order to assess the state of health of individuals. At airports, passengers are already being registered by smart video surveillance systems, and facial recognition using heat sensing cameras is being implemented at gates in order to measure higher temperatures and to single people out where necessary. The longer the pandemic lasts, the greater the risk of further invasion of people's privacy. This is the case in particular when sensitive data on the state of health of individuals are recorded and collected.

Data protection difficult to maintain

This means that the core problem of digitisation is exacerbated even more: the identifiability of people through technical means at any moment. It is becoming even more difficult to somehow maintain data protection. Biometrics links technology and the data it generates even more closely with identity. This makes the anonymous or pseudonymous use and separation of different applications that ensures that data cannot be linked extremely difficult.

Biometrics rapidly impacts human dignity

Technologies that use physical characteristics do not only violate our privacy more and more, they also impact human dignity.

Demands

- **Awareness of risks and action by the legislator**
  The immense risks posed by applications that record sensitive biometric data call for better protection. In the consumer sphere in particular, biometric applications are increasing and hence - due to the high market value of these data - the risk of wrongful use, identity theft and data misuse is rising significantly. The GDPR prohibits on principle the processing of biometric data and only allows these in strictly defined situations. However, these provisions fall way too short of dealing with risks and the possibility of misuse.

- **Biometrics must not become a commercial transaction**
  The commercialisation of and trading with biometric data and transfer to external third parties should be prohibited on principle and punished with more stringent penalties.

- **Freedom of choice is the top priority**
  Every consumer should be able to decide individually whether her/his biometric data can be processed or not.

- **Mandatory check before reaching for biometric data**
  In view of the high risks and potential damage related to misuse and wrongful use, a careful examination should be made before each use as to whether the processing of biometric data is necessary, sensible, and proportionate.

- **Clear restrictions on applications**
  Measured against the risks and dangers of misuse, from the viewpoint of consumer protection there is scarcely any potential for sensible applications with regard to end users. A possible application of biometrics is given

in the case of high security requirements, for example linking biometric characteristics to dangerous goods such as firearms. This could help to contribute, among others, reducing the misuse of firearms or other dangerous goods.

- **Strict rules for online banking**
  Specifically in terms of online banking no biometric data or their digital components (hash values, etc.) should be stored long-term.

- **Compulsory security standards**
  Whenever biometrics are used as an additional authentication factor, for example in online banking, care should be taken to protect data from external access and that biometric data or their digital components (hash values, etc.) are not stored long-term.

- **Prohibition of discrimination**
  Supporting the prohibition of discrimination by official preliminary examinations

- **Photographs of faces should always be treated as sensitive data**
  Photos of faces are already being used in numerous cases to identify people through facial identification. In view of the technical possibilities offered by AI, facial photographs should always be treated as biometric, sensitive data that therefore should be given special protection.

- **Identification vs. Authentication**
  Prohibition of identification when authentication is sufficient

- **Long term storage of data**
  Procedures that do not store biometric data long-term should be prioritised

- **Penalties**
  Violations of data protection and security standards must be penalised more severely

- **Harmonise rules**
  Currently there are significant gaps in regulations on facial recognition at the national, European, and international level. At the international level more stringent regulations on facial recognition and biometrics could be considered within the framework of Convention 108. Convention 108 was updated in 2018 and since then contains provisions on biometric data and algorithms.

- **Strict rules on facial recognition**
  Facial recognition is a technology that, in today's terms, poses the greatest threat to fundamental rights and democracy. Technical shortcomings, such as extremely high error ratios, technically aggravated discrimination, racism, suppression, mass surveillance and the loss of privacy, anonymity and personal freedom, are grounds enough to establish strict legal limits. This includes: the prohibition of real-time surveillance; allowing facial recognition in videos only in rare cases by way of exception and subject to the strictest requirements; prohibition of fully automated comparison of facial images from wanted persons databases to identify suspects, since the high error ratios associated with facial recognition generate many false positives, with considerable negative consequences for those affected.

Literature

Institute of Technology Assessment (ITA): Der Körper als Schlüssel? - Biometrische Methoden für Konsument:innen (german only)

European Data Protection Supervisor (EDPS): Facial Emotion Recognition, TechDispatch #1/2021

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK): Positionspapier zur biometrischen Analyse, 2019 (german only)

Authors

Daniela Zimmer
daniela.zimmer@akwien.at

September 2021

AK EUROPA

The Austrian Federal Chamber of Labour is by law representing the interests of about 3.8 million employees and consumers in Austria. The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.