TECHNOLOGY BRIEF

eu-LISA

BIOMETRIC TECHNOLOGY ···· PART 1

A PARADIGM SHIFT IN IDENTITY MANAGEMENT AND SECURITY TECHNOLOGIES

"Every human being carries with him from his cradle to his grave certain physical marks which do not change their character, and by which he can always be identified--and that without shade of doubt or question."

Mark Twain, "The Tragedy of Pudd'nhead Wilson", 1893

Automated biometric recognition technology, or simply 'biometrics', appeared in the 1960s as a paradigm shift to the classical security and identity management technologies used until then. With these new systems, one is not recognised by something that they know (e.g., PIN or password) or something that they possess (e.g., passport, key), but by something that they are (e.g., face, fingerprints). This makes biometric technologies more challenging to abuse than traditional methods of identification as, unlike passwords or ID cards, biometric identifiers are difficult to guess, share, misplace, copy or forge. This way, behind the catchy slogan 'you are your own key', biometrics have continuously grown since their inception, becoming nowadays an integral part of our daily lives.

WHAT IS BIOMETRICS?

Experts in law enforcement and forensics had developed manual methods for recognising individuals based on their behavioural and biological characteristics as early as the 19th century. Although earlier works on biometrics exist, Sir Francis Galton is widely recognised as the 'father' of fingerprint recognition. His landmark publication, Finger Prints, published in 1892 , is often cited as the first scientific treatise on biometric recognition.

In contrast, automated biometric systems, have only become available over the last half-century, due to the significant advances in the field of computer processing. Many of these automated techniques, however, are still based on the ideas originally conceived by the pioneers of biometric science, such as Galton.

Nowadays, and for the purpose of this technology brief, the domain of biometric recognition can be simply defined as an area of science and technology that studies the automated recognition of individuals based on their biometric characteristics.

WHAT IS A BIOMETRIC CHARACTERISTIC?

A biometric characteristic is understood as a biological and/or behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of recognition. Examples of biometric characteristics are: fingerprint-ridge structure, facial-skin texture, facial topography, hand geometry, iris structure, vein pattern of the hand, ridge structure of the palm, handwritten signature dynamics, handwritten signature pattern, voice signal, and gait.

WHAT IS THE BEST BIOMETRIC CHARACTERISTIC?

With so many biometric characteristics having been analysed by scientists and industry, a critical point is the choice of the biometric characteristic(s) to be used for each specific use case. From a pure technological perspective, the choice of a biometric characteristic for a particular application usually depends on the degree to which the following properties are satisfied:

1.UNIQUENESS (also referred to as distinctiveness). The characteristic should be sufficiently different for individuals in the relevant population to be distinguished from one another in an automated way. The level of uniqueness should also be as uniform as possible across the population to avoid biases associated with demographics.

1. In this technology brief, we have tried to minimise references to technical terminology. However, for the interested reader, definitions are provided in the harmonised biometric vocabulary available in the ISO/IEC 2382-37:2022 standard.

2.Francis Galton, Finger prints, Macmillan, 1892.

2.PERMANENCE. Ideally, a biometric characteristic, or its digital representation ultimately used for recognition purposes (i.e., the extracted features that conform to the biometric template), should change as little as possible over the lifetime of an individual, and should retain its discriminatory power (i.e., distinctiveness).

3.UNIVERSALITY. Every person should possess the characteristic.

4.COLLECTABILITY. High-quality samples of the biometric characteristic should be easy to acquire in an automatic and repeatable way, with as little intervention as possible (ideally none) from an expert.

5.PERFORMANCE. The distinctiveness of the characteristic is the key determining factor regarding the recognition accuracy of the final system. However, while minimising the recognition errors remains at the forefront of the performance attributes of a given system, other important performance measures also need to be taken into account, such as processing/response time, processing power and budget.

6.ACCEPTABILITY. Individuals in the relevant population should be accepting of the technology and be willing to have their biometric characteristic captured and assessed for recognition purposes.

7.INVULNERABILITY. The biometric characteristic should be robust against potential attacks and should be difficult to covertly acquire and/or forge.

8.INTEGRATION. Finally, the biometric characteristic should allow for a fairly seamless integration within the final system, for both operators and users.

There is no perfect, fit-for-all, biometric characteristic. Depending on the context and purpose of the deployment, the owner of the system may want to favour security/accuracy over convenience for the user, or vice versa. For instance, to acknowledge the receipt of a package, we may select a biometric trait with high user acceptability and collectability, such as a handwritten signature, at the cost of lower accuracy and higher vulnerability. On the other hand, to get access to a high-security safe box in a bank, accuracy should be the prime factor by opting for a combination of highly accurate biometric characteristics, such as all 10 fingerprints together with an iris scan, even if acquisition time, collectability and general convenience for the user are compromised.

The two most deployed, analysed and developed biometric characteristics are fingerprints and face. Both characteristics are now present in many daily applications, such as when accessing digital devices (e.g., unlocking smartphones). They are also widely used in border management and law enforcement, where a combination of fingerprints and the facial image have proven to be a good trade-off between accuracy (security), collectability (convenience for travellers, in terms of both easiness of acquisition and acquisition time), and processing speed.

WHAT ARE THE BENEFITS OF BIOMETRICS?

Unlike other forms of identity management technologies, biometric characteristics are inherently linked to a person's identity from birth. This property comes with a number of advantages, such as:

CONVENIENCE. 
Biometric characteristics are more difficult to forge, copy, forget and misplace than, for instance, passwords, PINs, identity cards or digital credentials. This makes biometrics very convenient for uses such as physical access control and logging in to digital devices. It also allows for a more seamless and speedier travel experience, where the traveller can self-prove their identity at self-service kiosks without needing to wait in line or interact with border guards.

NEGATIVE RECOGNITION. 
One of the most powerful properties of biometric technology is that it allows for negative recognition and, therefore, the detection of biographical identity theft/fraud. Even when in possession of a valid identity document (e.g., a stolen passport), biometric checks make it possible to verify whether a person is who they claim to be or, on the contrary, whether they are claiming to be someone they are not.

IDENTITY DEDUPLICATION. 
Biometrics make it possible to detect when biographical identities are duplicated. Biometric databases enable authorities to detect if someone is already present in a system under a different biographical identity (e.g., name, surname, passport number) or if they are matching multiple biographical identities to the same biometric identity.

WATCH LISTS. Biometrics allow for fast searches in watch lists. Even if a person being searched presents a document with different biographical data, biometrics enable authorities to search and find the person in real time in large watch lists.

LAW ENFORCEMENT INVESTIGATION. Biometrics provide further means of investigation for law enforcement. In the law enforcement and forensic fields, biometrics is often the only identity data available when, for instance, searching for a missing person, identifying a corpse, or examining a crime scene. As a concrete example, the use of biometrics is unlikely to find a paper or digital identity document at a crime scene, but a CCTV camera can capture an image of the criminal's face[3], or the criminal may leave traces of their fingerprints[4] (i.e., finger -marks).

WHAT ARE THE LIMITATIONS OF BIOMETRICS?

Just like any other identity management and security technology, biometrics is not perfect. Some limitations and challenges should also be acknowledged:

VULNERABILITY. Just like any other security and/or identity management technology, biometrics may be exposed to potential attacks. In addition to the digital cybersecurity risks common to other IT-related digital technologies, some threats are specific to biometrics, namely presentation attacks and morphing attacks. In classical presentation attacks, an ill-intentioned individual uses an item (e.g., rubber fingertips, face mask) that mimics the biometric characteristic of the legitimate user to impersonate them and gain access to the system. In the case of a typical morphing attack, two accomplices generate a biometric synthetic composite sample (e.g., facial image) that positively matches the original biometric characteristics of both individuals. This composite image is then enrolled into a system (e.g., stored in a biometric passport), so that both persons can have access to the system using the same identity. The consequences of a successful attack leading to a security breach of a biometric system can have more serious consequences than for other traditional security technologies, due to the high linkability and limited renewability of biometric characteristics.

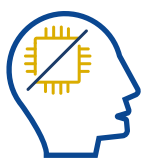
LINKABILITY. Biometrics being immutably linked to each individual is a double-edged sword: while it allows for the detection of identity duplication, identity fraud and identity theft, if used incorrectly it also makes it possible to track a legitimate user through different systems originally designed for different purposes, which may have a major impact on personal privacy.

We can enable different traditional access credentials, linked to our identity, to be used in different systems (e.g., a different password or PIN for each system/application). This way, if one of those credentials is compromised, the potential damage is limited to the specific system for which it was issued. With traditional identity management approaches, our identity cannot be linked across systems. This is not the case for biometrics. If, for instance, our facial image is compromised, it can potentially be used by criminals to track our activities or gain unauthorised access to any system in which our facial image has been enrolled.

RENEWABILITY. As mentioned above, passwords, PINs, keys and digital credentials can be re-issued if they are compromised, but this is not the case for biometric data. We cannot get a second right index finger if the first one is 'stolen' by a criminal.

VARIABILITY. The accuracy of traditional identity management systems is based on deterministic data, thus can be mathematically determined to guarantee consistency across the entire population. In biometrics, however, due to its intrinsic statistical nature (two fingerprint images of the same finger are never the same, but 'somewhat' similar), accuracy cannot be ensured, as it will change depending on the consistency between training and test data, in terms of both representativeness of the population and quality of the data.

BIAS. The sources of data variability mentioned in the previous point can be linked to external acquisition factors (e.g., illumination conditions), but can also be intrinsic to the diversity among different segments of the population. This can lead to performance biases of biometric technology with respect to demographic groups. For instance, a speaker recognition algorithm



3. Face recognition and the Boston Marathon bombing suspects.
4. Fingerprint recognition and a 30-year-old murder solved.

may be better suited to discern among voices with a higher pitch, which will lead to better accuracy among women than men. Similarly, if the data used to train a facial recognition algorithm is skewed towards the Asian population, the system will have lower recognition error rates when dealing with individuals of that ethnicity than, for example, Caucasians.

HOW IS RESEARCH AND INNOVATION ADDRESSING BIOMETRICS LIMITATIONS?

Both the scientific community and industry are devoting substantial resources to address some of the existing limitations of biometrics. In particular, open areas that are currently being developed are:

ATTACK DETECTION. Automatic approaches are currently being developed and integrated into operational biometric systems to detect and flag attack attempts from bona fide attempts. While such techniques, studied in the literature in the fields of presentation attack detection (PAD) and morphing attack detection (MAD), are still somewhat imperfect, they do provide an extra layer of protection that enhances the overall security offered by biometrics.

DEEP LEARNING. The advent of deep learning (DL) approximately a decade ago has been a game changer in the development of image processing technology, machine learning and pattern recognition. As a result, the impact of deep learning on all areas of biometric recognition technology has been outstanding. This performance-boosting effect has been especially groundbreaking in the particular case of facial recognition, where error rates have dropped by a factor of approximately 100 since 2014 with the appearance of the first deep-learning implementations, as shown by the results obtained by current DL-based facial recognition algorithms participating in the independent competitive evaluation organised by the US National Institute for Standards and Technology (NIST) – the Face Recognition Technology Evaluation[5] (FRTE). This exponential improvement in accuracy and performance is only expected to continue into the future, with the constant progress of deep-learning algorithms, the availability of training data, and computer processing power.

DATA QUALITY ESTIMATION. As mentioned above, the accuracy of biometric systems is largely dependent on the quality of the data they run on. As such, a lot of effort is being put into developing automatic algorithms that can predict to what extent a specific biometric sample will provide high accuracy for recognition purposes. Two examples of successful collaborative initiatives to implement quality estimation algorithms are NFIQ2[6] for fingerprints and OFIQ[7] for the face. Both quality measures are standardised, vendor-independent and open-source, which makes them especially valuable for the interoperability of biometric systems.

ACQUISITION UNDER UNCONTROLLED CONDITIONS. As a general rule, highly controlled acquisition conditions (such as those found in law enforcement facilities) result in high-quality biometric data and, in turn, very low error rates. In contrast, unconstrained acquisition scenarios (e.g., an outdoor selfie or CCTV footage) provide biometric data of degraded quality and, therefore, high error rates. A lot of investment is currently being put into improving the overall performance of biometric technology when the acquisition conditions are sub-optimal.

BIOMETRIC READERS. Data quality is mainly determined at the time of acquisition. Overall, three types of factors play a role during acquisition: environmental (e.g., temperature or illumination), behavioural (i.e., how the user interacts with the acquisition device), and the biometric scanner itself. Improvements in biometric acquisition devices, both from a usability/ergonomics perspective and from the sensor technology used, can definitely help to improve the final overall quality of the acquired data for a given set of (uncontrollable) environmental conditions. As such, efforts are afoot to design and develop better biometric readers, such as the new trend of touchless fingerprint scanners that could potentially help to improve the quality of the acquired data for certain segments of the population, such as elderly people. As we grow older, our skin becomes less elastic and dryer, and therefore less suitable for interactions with traditional fingerprint touch-based scanners. Consequently, elderly people could greatly benefit from the new generation of contactless technology.

MULTIBIOMETRICS. As already mentioned, there is no 'one biometric characteristic to rule them all'. Improved, more uniform and more consistent overall performance can be achieved if different biometric characteristics are combined, so that each of them accounts for or complements the potential flaws of the others. This trend, which also includes the use of different sensors to capture the same characteristic (e.g., the face being captured with a visual-spectrum sensor and a thermal sensor), is referred to as multibiometrics,

5.NIST, Face Recognition Technology Evaluations – FRTE/FATE.
6.NIST, Fingerprint Image Quality (NFIQ 2).
7.BSI, Open Source Face Image Quality (OFIQ).

and is a highly studied area within biometrics that can provide improvements to some of the limitations of the technology.

BIOMETRIC ENCRYPTION. Another very active area of work within biometrics is the development of encryption solutions that are specifically designed for the particular challenges posed by biometric statistical data. These new applications, which are generally grouped under the umbrella of the so-called biometric template protection (BTP) schemes, can help to provide a by-design answer to the current renewability and linkability limitations of biometrics as presented above.
At the cost of adding an extra layer of complexity, the goal of BTP approaches is to circumvent the one-to-one univocal correspondence between the biometric sample (e.g., fingerprint image, facial image) and the biometric template (i.e., digital encoding of the biometric sample), as exists in traditional biometric systems[8], while maintaining all the other advantageous features. In essence, these techniques make it possible to produce different non-matching (i.e., unlinkable) biometric templates from one unique biometric sample. If this objective were reached, it would constitute a breakthrough in the enhancement of the privacy level provided by the technology.

EVALUATION. Just as important as identifying the areas where a specific technology can (and should) be improved, is the ability to objectively quantify its limitations, in order to clearly keep track of progress. For this reason, the biometric community is continuously investing in the development of standardised evaluation frameworks (including metrics, protocols and guidelines) to fairly assess key performance indicators of biometric systems such as accuracy[9], linkability[10], vulnerability[11], bia[12] and quality[13].

STANDARDISATION. One key area that can provide a big boost towards developing the next generation of biometric systems is the promotion of standardisation. The standardisation process brings together all key players involved in biometrics: academia/scientists, industry, end users (e.g., law enforcement and border management agencies) and policymakers. Having joint agreements on definitions, evaluation frameworks and communication formats is a very powerful tool in eventually overcoming some of the limitations of the technology.

HOW ACCURATE ARE BIOMETRICS?

Even though this may seem like a fairly simple question, there is no straightforward answer to it. As already pointed out, the accuracy of biometric recognition is fully dependent on the type of data that a system runs on, which, in turn, is determined by factors such as population, operational environment or type of application, and use case. This way, two identical recognition systems may present error rates that differ from each other by a factor of more than 10, depending on the aforementioned criteria.

This is why, when performing operational evaluations of biometric systems, following standardised guidelines and good practices is of the utmost importance for any organisation that relies on this technology for its business.

With those caveats in mind, and solely for the purpose of providing a general overview of the order of magnitude of error rates that current biometric recognition systems are capable of achieving, we will present here some accuracy[14] figures for one of the most commonly deployed biometric characteristics: the face.

The error rates have been extracted from the latest evaluation performed by the US NIST. NIST is the most reliable source worldwide of vendor-independent competitive biometric assessment, having been conducting such evaluations for over two decades. NIST is currently performing a Face Recognition Technology Evaluation (FRTE), and in its most recent results report, dating from February 2024, the best facial recognition algorithms have achieved the accuracy performance reported in figure 1 for some of the most representative scenarios considered. These results clearly showcase the huge dependency of biometric recognition accuracy with the quality of the data captured. The results reported in the NIST FRTE evaluation presented below show a 50-time accuracy difference between scenario 1 (in which both images are captured in fully controlled conditions, i.e., visa images acquired in a supervised

8.For a quick overview of the different general modules and their respective inputs/outputs (such as biometric samples and biometric templates) that conform a classical biometric system, we refer interested readers to Chapter 1: Introduction to biometrics of the 'Handbook of Biometrics' (Springer, 2008).

9.ISO/IEC 19795-1:2021. Biometric performance testing and reporting – Part 1: Principles and framework.

10.ISO/IEC 30136:2018. Performance testing of biometric template protection schemes.

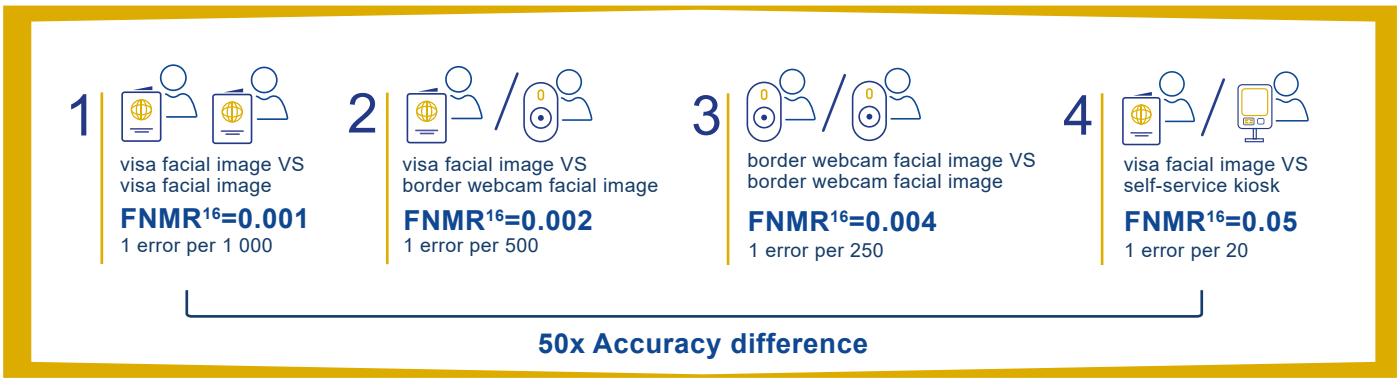
11.ISO/IEC 30107-1:2023. Biometric presentation attack detection – Part 1: Framework.

12.'Fairness Index Measures to Evaluate Bias in Biometric Recognition'.

13.'Considerations on the Evaluation of Biometric Quality Assessment Algorithms'.

14.For a technical and precise definition of the metrics used in biometric accuracy testing and reporting, we refer interested readers to the ISO/IEC 19795-1:2021 standard.

Fig.1. Face VERIFICATION scenarios ("1vs1" comparison, for an FMR[15] of 1 error per



environment), and scenario 4 (where one of the images is captured in uncontrolled conditions, i.e., at a self-service kiosk).

WHERE ARE BIOMETRICS USED?

Historically, applications using biometrics have been driven by criminal investigation authorities and for civil identification and military purposes, under a very strict legal and technical framework. However, starting from those initial use cases, biometrics have evolved and been applied to many other different fields including banking, healthcare and digital commerce. Over the last decade, awareness and acceptance of biometric technology by the general public have been boosted thanks to its integration for unlocking and logging in on smartphones, tablets and laptops, usually by means of a fingerprint and/or facial recognition.

Nowadays, biometrics are generally deployed in any area where identity management is required. As such, some of the domains that benefit the most of the advantages offered by this technology are:

Border management, travel and migration control, e.g., identity management of travellers, passengers, migrants and asylum seekers. In this context, biometrics play a key role in implementing a more seamless experience for travellers through the use of the biometric passport, biometric-enabled ABC gates at border crossing points, and biometric self-service kiosks for enrolment on border management IT systems.

Civil ID management, e.g., identity management of citizens, residents, voters and taxpayers. Biometrics have become a key technology for remote communication between citizens and government authorities.

Law enforcement, public security and the judicial system, e.g., identity management of missing persons, wanted persons, criminals, suspects, wrongly accused persons and unidentified deceased persons.

Healthcare, e.g., identity management of patients, beneficiaries of the healthcare system, and healthcare professionals.

Physical and logical access, e.g., identity management of owners, users, employers, employees, and persons with access rights.

Commercial applications, e.g., identity management of customers, sellers and buyers.

WHY ARE BIOMETRICS CONTROVERSIAL?

As presented so far, the advantages offered by biometrics are significant for both service providers and service users. However, there is still some resistance to the full adoption of this technology in society. In spite of its ubiquitous presence, biometric recognition systems are still perceived with a certain general sense of unreliability and untrustworthiness.

Although some of the early myths surrounding biometrics and the possibility of building a 'big brother' society have now been largely debunked in Western democracies, there are still some legitimate concerns regarding the misuse of biometrics among not only the general population, but also – and perhaps more importantly – regulators and policymakers.

These concerns are mainly related to privacy, citizens' ability to control their data and information, and potential discrimination stemming from biases in the performance of biometric systems with respect to different demographic groups. In general, three types of risks are identified:

15.FMR stands for False Match Rate. It defines the number of errors that the system makes when comparing two samples from different persons. FMR=10-6 implies that, on average, 1 time every 1 million comparisons of two samples (e.g., facial images) of different persons the system considers they belong to the same person.

16.FNMR stands for False Non-Match Rate. It defines the number of errors that the system makes when comparing two samples from the same person. FMR=0.001 implies that, on average, 1 time every 1 000 comparisons of two samples (e.g., facial images) of the same person the system considers they belong to different persons.

UNINTENDED USE. The risk of biometric data being uses for purposes other than those agreed by the citizen, either by service providers or fraudsters and whether private (e.g., multinational companies) or public (e.g., governments, law enforcement agencies). As soon as biometric data is in the hands of a third party, there is a risk that it may be used for purposes other than those for which the person concerned gave their consent. Thus, there may be cases of unwanted end use if such data is interconnected with other files or used for types of processing other than those initially intended.

LINKABILITY. As already highlighted above, one of the limitations of the technology is the risk the data presented for biometric checks being reused. The data may be captured during transmission or extracted from a database, and fraudulently replicated or used to gain access to different services.

BIAS. Lately, the general public have echoed some legitimate concerns raised by different sectors within the biometric community regarding the potential discrimination that this technology may bring due to differences in its performance with regard to specific population profiles (e.g., related to age or gender). Such divergence with respect to the desirable equal treatment of all citizens is not an issue unique to biometrics, but it can be observed even in human-driven processes. However, several blatant cases reported in a somewhat sensationalist manner in the press have put the technology under a lot of scrutiny in this regard[17],[18].
As mentioned above, bias is one of the limitations currently being addressed in biometrics in order to detect it, to properly asses it and to apply the necessary corrective measures.

CONCLUSION

It has now been clearly established over several decades of extensive usage in multiple domains, that the advantages that biometric recognition systems bring to the field of identity management decidedly outweigh their limitations. This does not mean that all concerns regarding this thriving technology have been solved. However, there is an unquestionable commitment and investment from all parties involved in the development of biometric systems, to address their downsides and provide innovative solutions to existing shortcomings. From researchers to regulators, public authorities, end users and industry, a strong joint effort is being made to bring a new generation of improved biometric applications that can keep providing added value to citizens.

Given the current state of play laid out in this technology brief, the advancement of biometrics and its full acceptance will be largely dependent on three key parameters:

REGULATION. As with any innovation, it is important to regulate the use cases in which this technology is employed, to properly define the boundaries of its operation. I It is essential to analyse and understand this potential negative impact, in order to avoid it with the necessary preventive measures, not only through regulatory safeguards like the AI Act[19] that puts strict limits to the use of real-time and remote biometric recognition, but also by promoting good practices and concrete guidelines[20,21] for the proper, respectful and righteous use of biometrics. Likewise, it is necessary to put in place the necessary supervision mechanisms, to detect any possible cases of abuse of the technology, which should result in clear punitive actions.

TRAINING. It is also essential to provide proper training to professionals using the technology (e.g., border guards, law enforcement, forensic examiners), so that they are well aware of how to properly use it, what it is capable of offering and how to interpret its outcome.

EDUCATION. Raising public awareness of the new technology and being transparent on its use and protections provided for their privacy, will be the only way to achieve acceptance of biometrics among the majority of society, and to eliminate some of the existing fears of it.

As far as privacy objections are concerned, government regulation and public education will be required if full acceptance of the technology is to be achieved. As is the case for many other technologies, especially dealing with personal information, trust needs to be built through regulation and education.

In summary, not only the full biometrics community, but also society as a whole, need to work together to get the most out of the great potential that this technology has to offer, because, like it or loathe it, biometrics is here to stay.

17. 'Uber eats settles driver's facial recognition discrimination claim'.
18. 'Police Facial Recognition Technology Can't Tell Black People Apart'.
19. AI Act.
20. Council of Europe, "Guidelines on facial recognition"
21. Biometrics Institute, "Biometrics good practice guidance"

TECHNOLOGY BRIEF

eu-LISA

Technology Brief completed in June 2024
Neither eu-LISA nor any person acting on behalf of eu-LISA is responsible for the use that might be made of the following information.
Luxembourg: Publications Office of the European Union, 2024

ISBN 978-92-95227-89-7
ISSN 2812-0795 doi:10.2857/354390
Catalogue number: EL-AW-24-001-EN-N

© eu-LISA, 2024
Reproduction is authorised provided the source is acknowledged.
For any use or reproduction of elements that are not owned by eu-LISA, permission may need to be sought directly from the respective rightholders. eu-LISA does not own the copyright in relation to the following elements: