Biometrics, surveillance and privacy

ERNCIP Thematic Group Applied Biometrics for the Security of Critical Infrastructure

Max Snijder
European Biometrics Group, the Netherlands

2016

REPORT EUR 28389 EN

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

Biometrics, surveillance and privacy

This publication is a technical report by the Joint Research Centre, the European Commission's in-house science service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC Science Hub
https://ec.europa.eu/jrc

JRC104392

EUR 28389 EN

ISBN 978-92-79-64822-9

ISSN 1831-9424

doi:10.2788/986068

.

Contents

1. Introduction 2

2. Background 3

3. Areas of concern for EU stakeholders on preserving the privacy of citizens, arising from the collection, storage and use of biometric data 4

3.1. Increased surveillance for the protection of EU citizens: impact on the privacy/security balance 4

3.2. Biometrics and privacy 5

3.3. Cyber biometrics and private sources: anonymity on the internet and in public spaces 6

3.4. EU data protection reform and existing work of Article 29 working party 8

3.5. Data protection by design and by default 10

3.6. Biometrics and CCTV 11

4. Findings and conclusions 13

5. Recommendations 14

5.1. General recommendations 14

5.2. Recommendations for future work of the Biometrics thematic group 14

1. Introduction

There are a number of issues associated with privacy and biometrics that will need to be addressed for successful and responsible implementation of biometric technology. This report will articulate these issues, explore their impact and identify any activity needed to address them. This will be done at a general level, while sometimes reference is made to the new international standard for video surveillance systems (VSS) using biometrics, ISO 30137 (Full title: 'Information technology — Use of biometrics in video surveillance systems'), which is currently under development. This draft standard consists of the following parts:

— Part 1: Design and specification
— Part 2: Performance testing and reporting
— Part 3: Data formats
— Part 4: Ground truth and video annotation procedure

Part 1, ISO 30137-1, was prepared by Technical Committee ISO/IEC JTC1 Subcommittee SC 37, Biometrics and has been provided to the ERNCIP Thematic Group Applied Biometrics for input and comments. References made only concern Part 1 of the standard.

This report is intended to encourage discussion and debate regarding the development of legally and ethically sound policies and systems. It is not meant to be a comprehensive and elaborated study given the scope of the assignment.

Biometrics and identity management are becoming increasingly important in securing European society. This is due to the strong growth of mobility accelerated by globalisation and geopolitical changes, such as immigration and the digital economy. We are finding biometrics in a broad range of applications, such as the e-Passport, automated border control, immigration control, law enforcement, financial services, various smartphone-based applications and video surveillance.

New technical possibilities are turning into innovative solutions in ever shorter time frames, sometimes exceeding societies' ability to adapt those solutions in a responsible and thoughtful way in the democratic processes and law-making. It is the digitisation of our society that provides new ways of living, but also creates new challenges in maintaining security and privacy in a transparent way. In this context we can consider biometrics as an ultimate exponent of these developments: systems with improved computing powers, unlimited connectivity and highly sophisticated sensors and algorithms are now capable of performing large-scale identification, verification and authentication functions for a variety of purposes, whether overtly or covertly.

This report describes why biometrics confronts us with profound challenges regarding the protection of citizens' data and associated privacy concerns due to the collection and sharing of such data by private entities (such as search engines, credit registrars, data brokers, web shops, website trackers and optimisers, social media, chambers of commerce, health care institutions) and public entities (such as tax authorities, public administrations, driver licence authorities, social care agencies, and police and justice authorities).

2. Background

Stakeholders in the critical infrastructure protection (CIP) ecosystem are especially mindful of continually improving the security of systems (such as those individuals responsible for security at airports and for secure water supplies, nuclear facilities, energy plants) as well as those who deliver on those security requirements. Protection providers can be public parties (e.g. police, intelligence, military and justice authorities) and private parties (e.g. security firms, system providers). These stakeholders have posed a series of security and privacy challenges that will need to be addressed by biometrics and/or other security technologies. Biometrics has capabilities that are difficult to replicate in other ways and are presenting challenges that need to be addressed to use them successfully. These challenges have been highlighted and are being addressed in a number of ongoing standards activities and initiatives such as this ERNCIP Thematic Group (TG) on Biometrics.

During the past 2 years the ERNCIP Thematic Group Applied Biometrics for the Security of Critical Infrastructures has (amongst other work) put effort into providing input to the abovementioned new international standard on VSS using biometrics, ISO 30137-1. This report, which is at Committee draft stage at the time of writing of this report, will occasionally take this draft standard as a reference for certain aspects of the discussion.

There are a number of issues associated with privacy and biometrics that need to be addressed for successful implementation of biometric technology. This report will set out these issues, explore their impact and identify activities needed to address them. This will be partly done at a general level and partly by using the abovementioned new VSS Standard as a reference.

3. Areas of concern for EU stakeholders on preserving the privacy of citizens, arising from the collection, storage and use of biometric data

3.1. Increased surveillance for the protection of EU citizens: impact on the privacy/security balance

Biometrics and identity management are becoming increasingly important in securing European society. This is due to the strong growth of mobility accelerated by globalisation and geopolitical changes, such as immigration and the digital economy. We are finding biometrics in a broad range of applications, such as the e-Passport, automated border control, immigration control, law enforcement, financial services, various smartphone-based applications, video surveillance and digital identity online.

Biometric characteristics can be very discriminative for each individual. As a result, biometric technology can bind an identity to a body of a person, rather than to what this person may know or have in his/her possession. Its discriminative potential determines the risk in relying on that binding. Within the statistical boundaries that are inherent to the use of biometrics for identification and authentication purposes, we can say that in the applications mentioned above, identity assurance through biometrics is becoming a key enabler to achieve improved levels of convenience, security, availability and efficiency that are difficult, if not impossible, to achieve by other means.

We are living in an era where computing capacity and the availability of wireless networks are expanding in an unprecedented way. New technical possibilities are turning into innovative solutions in ever shorter time frames, sometimes exceeding society's ability to deploy those solutions in a responsible and thoughtful way with regard to democratic processes and law-making. The increasing complexity of these new technologies also can lead to a situation where a knowledge gap occurs between those who develop and deploy the technologies and those who need to ensure that this happens in a responsible and accountable way, such as civil society, regulators, independent advocates and operators. In other words, the risk emerges that lawmakers, data protection authorities and associated legal systems are not able to cope with the technical progress and can't properly assess current and future risks of using these technologies for our free societies.

At the same time we see external threats such as terrorism, cross-border organised crime and complex issues like immigration, which urgently require measures that prevent disasters from happening. Here we see that new state-of-the-art technologies come into play, such as highly sophisticated systems that literally keep a close eye on our physical and digital world. It is the digitisation of our society that provides new ways of living, but also creates new challenges in maintaining security and privacy in a transparent way. In this context we can consider biometrics as an ultimate exponent of these developments: systems making use of improved computing power, unlimited connectivity and highly sophisticated sensors and algorithms are now capable of performing large-scale identification, verification and authentication functions for a variety of purposes. In the context of this report we shall focus on the use of biometrics for video surveillance systems (VSS) applications (such as closed circuit television (CCTV) systems), although some other state-of-the-art biometric applications will also be discussed.

3.2. Biometrics and privacy

Biometric information is derived from the discriminative characteristics of a person's body or his/her behaviour. The operational format of biometric information is the digitised template to 'import' a physical representation of a person into an otherwise fully digital environment. The discriminative properties of this representation may depend on the kind of physical characteristic that has been measured. For example: in certain cases an iris may contain more discriminative information than a fingerprint. The usability of biometric information is also not the same for all modalities. If cameras are available, facial recognition may be the most practical, while on a desktop computer without a camera, keystroke dynamics may be the preferred choice. Whatever modality is chosen, it will be the digital representation of the human characteristic that will be used for identification (1:n) and verification (1:1) purposes. This feature of biometrics is unique and can't be replaced by any other technology currently available. As a result the human body becomes a powerful tool for distinguishing between people and deciding whether or not a person belongs to a certain predefined group (e.g. a watch list). This can be for inclusion as well as for exclusion. As such, biometric systems are discriminative based on the decision of a biometric comparison process. This process is based on statistical analysis and has an intrinsic potential of failures. These failures — if detected — can have a variety of causes and will typically result in the need for human intervention at some stage in the process, either real time or off line.

An important feature of biometrics is that in most cases biometric data cannot be considered to be secret. A picture in a passport is hardly a secret, as long as a face is carried in the open and in many cases it may be uploaded to public sites such as Facebook, Picasa and LinkedIn. As a result, biometrics cannot be treated strictly as a person's secret from a practical and legal point of view. At the same time, it is now ruled in the EU under the new general data protection regulation that biometric data are personal and **'present specific risks to the rights and freedoms of data subjects by virtue of their nature'** ([1]).

Assessing various elements of a specific application, such as purpose of the application, management of the data and the potential of linking the biometric data to other systems will be important factors in determining the sensitivity of the biometric data, and therefore the legality of a certain application. This means that the assessment of the privacy aspects of a biometric application largely depends on how the biometric data are being used and managed. In order to do such an assessment adequately a minimum level of transparency must be available, while the functionalities of an application need to be frozen. If functionalities are changing over time a new assessment needs to be done. In addition, there needs to be a clearly defined process which informs the data subject about any extension of the use of the biometric data. From a legal and data protection point of view this could make biometrics a moving target: the facial images in an application may be legal at time X, while at time Y, after functionalities have changed, the same application may be assessed as illegal. In the context of privacy by design, as described in Article 30(3) of the European general data protection regulation (see also paragraph 3.4 of this report) this means that 'design' should be interpreted as a dynamic process, demanding legal reviews through the use of a data protection impact assessment (DPIA) at various stages of the life cycle of an application. It is for this reason, that already at the stage of conception of a standard (such as the draft VSS standard ISO 30137-1) data protection assessments are needed.

([1]) Article 33 'Data protection impact assessment' of the General Data Protection Regulation (see also Paragraph 3.4 of this report).

It is acknowledged that the existence of large-scale information systems, certainly if they store, process and use biometric data, also implies potential privacy issues, which need to be anticipated and addressed appropriately. The collection and use of personal data in these systems has an impact on the right to the privacy and the protection of personal data, enshrined in the Charter of Fundamental Rights of the European Union ([2]). In practice that means that all systems need to comply with data protection principles and requirements such as necessity, proportionality, purpose limitation and quality of data. Safeguards must be in place to ensure the rights of the data subjects in relation to the protection of their private life and personal data. It should be noted that the scenarios that involve the identity management of criminals and citizens are governed by different legal frameworks. It remains a challenge to develop parallel processes ensuring privacy and data protection for both groups of data subjects, while at the same certain overlap between these processes will need to exist as the criminals are a subset of the citizens.

'Data protection by design' and 'Data protection by default' are now principles of EU data protection instruments. When developing new instruments that rely on the use of information technology and personal data (such as biometric data), the Commission may seek to follow this approach. This implies embedding personal data protection in the technological basis of a proposed instrument, such as secure data storage and management. As low biometric quality significantly raises failure rates and therefore increases the number of mistakes and leads to reduced accuracy, which can result in accusing the wrong person or leaving crimes unsolved, quality and protection of biometric data are of key importance, certainly in case biometric references are being collected as a reference. This includes measures against spoofing of biometric data and reducing the chance that biometric evidence wrongly points in the direction of the victim (thus putting a victim of identity fraud into an even more difficult position in terms of proving his/her innocence). However, in law enforcement and policing, officers often have to take whatever latent fingerprints or CCTV images are available at crime scenes, thus they have no control over the quality of those biometric traces.

3.3. Cyber biometrics and private sources: anonymity on the internet and in public spaces

As discussed in the previous paragraph, biometrics are capable of 'importing' a digital representation of a physical person. Once this feature is being used in a purely digital context, we may speak about 'cyber biometrics'. With the introduction of biometrics for mobile devices such as smartphones, a strong impulse has been given to the development of sophisticated technologies for cyber biometrics. That includes the so-called classic biometric modalities (face, finger, voice, iris), but also new modalities that are based on people's behaviour in the cyber world, such as keystroke dynamics, voice, swipe dynamics (i.e. the way a person swipes the screen on a smartphone), dynamic signature, gait recognition (using the accelerometer of the smartphone) and others. Because the classic biometrics can be used in both the physical domain (e.g. border control, video surveillance) and the cyber domain, connections between these two domains can be established through these biometric features. So where removing anonymity on the internet by using biometrics for security reasons may be a legitimate objective (under specific conditions) to fight crime and fraud, it may lead to the removal of anonymity in public spaces as well, such as shopping centres and train stations.

When assessing the privacy risks of biometric-enabled CCTV systems it is important to understand whether the biometric information, which is derived from the cameras of such systems, are being

[2] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

linked to and/or enriched with data from other sources (such as Facebook, Google Face, Picasa, LinkedIn, public administrations) and if so, what the purpose and justifications are for such linking. Biometric data can link an individual to multiple systems and sources. So in case that biometric data are being captured and stored for a particular application, it is important that the actual usage of those data for other applications is transparent and consent is provided by the subject.

Increasingly, law enforcement, forensic and intelligence agencies are using a mix of private and public sources in order to establish identities or to follow people's traces. It is envisaged that this use of combined sources will develop into a mainstream practice ([3]). This trend takes us to the point that we need to take certain private sources of biometric information (e.g. GoogleFace, Facebook, Picasa, cloud-based authentication services, etc.) into consideration while recognising that these privately collected data are used in the law enforcement and intelligence domains. In practice this may result in the situation that mobile police officers, who carry webcams on their body, may not only be able to determine whether the person they are speaking with is a known or suspected criminal (through a connection to a watch-list), but in principle would also be able to establish the identity of any person whose faces they capture with the camera. The assumption here is that this mobile camera is connected to a central system, which collects biometric data from law enforcement sources as well as public sources as mentioned before. The same counts for surveillance of the internet and mobile networks with the emergence of cyber biometrics. An example of this practice is the US's Biometric Center of Excellence ([4]), which collects and organises biometric data from various sources with the purpose of making these available for general use by police, military and intelligence forces (inter-agency availability) to establish identity. That the controls and limitations that should protect the privacy and freedom of the data subjects can be put to the legal test, is illustrated by the court case that EPIC initiated against the biometric programme of the FBI (New Generation of Identification (NGI)) ([5]). Although there are legitimate reasons to use biometrics for the protection of national security and critical infrastructures, the public interest also demands adequate safeguards and controls. In an open government FOIA ([6]) case brought by EPIC against the FBI, a federal court ruled in EPIC's favour in 2014, finding:

'The dissemination of the material sought by EPIC, and the NGI system itself, are fairly within the public interest. The FBI's own website proclaims that its current fingerprint identification system is the largest in the world. The implications of expanding this system to include multimodal biometric data and interoperability with existing and future technology are of significant public interest, whether in the form of EPIC's concerns regarding liberty interests and privacy rights, the FBI's concerns with more effectively combatting terrorism and crime, or otherwise.
../..
There can be little dispute that the general public has a genuine, tangible interest in a system designed to store and manipulate significant quantities of its own biometric data, particularly given the great numbers of people from whom such data will be gathered.' ([7])

[3] 'Identity Management in 2030', Dutch National Office for Identity Data (2015).
[4] https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence
[5] https://epic.org/2016/11/epic-sues-fbi-over-biometric.html
[6] Freedom Of Information Act.
[7] https://epic.org/press/RELEASE-EPIC-Sues-FBI-11-15-16.pdf

Where data are also being gathered from various private systems such as Facebook and LinkedIn, it can happen that the biometric data are being used for purposes for which the data subject hasn't given his/her consent and which they may not be aware of. In such cases biometrics can link those private systems to government surveillance systems. The mass collection of biometric and other identity data is not restricted to (suspected) criminals and terrorists, but will also include citizens who are not under suspicion ([8]) ([9]). In some situations this results in the collection of the personal identifiers of large portions of a foreign population ([10]). These examples show the pivotal role and unique powers of biometric technologies in their ability to establish identity in large-scale surveillance systems, using a combination of various government systems and private systems.

3.4. EU data protection reform and existing work of Article 29 working party

When designing biometrics-based surveillance systems it is important to understand the context of the existing European privacy and data protection legislative environment. On 15 December 2015, the European Parliament and the Council agreed on the EU data protection reform. This reform consists of the following instruments:

— **The general data protection regulation** ([11]) will enable people to better control their personal data. At the same time modernised and unified rules will allow businesses to make the most of the opportunities of the digital single market by cutting red tape and benefiting from reinforced consumer trust.

— **The data protection directive** ([12]) for the police and criminal justice sector will ensure that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action. At the same time more harmonised laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe.

The **regulation** entered into force on 24 May 2016 and it shall apply from **25 May 2018**. The **directive** entered into force on 5 May 2016 and EU Member States have to transpose it into their national law by **6 May 2018**.

Because in modern surveillance public as well as private sources are being used for law enforcement, policing and intelligence purposes, both legislative instruments need to be taken into account when such surveillance systems are being designed and implemented.

Article 33 of the EU general data protection regulation (EU) 2016/679 mentions that both monitoring and specific data such as biometrics are posing a specific risk to the rights and freedoms of data subjects. According to the regulation that implies that 'the controller shall prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data'. In the case that surveillance systems are using biometrics (e.g. facial recognition), this specific risk will increase and the need for a data protection impact assessment (DPIA) and prior

[8] N.S.A. Collecting Millions of Faces From Web Images, Risen, Poitras, New York Times 2014.
[9] https://www.perpetuallineup.org
[10] https://publicintelligence.net/identity-dominance
[11] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[12] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN

authorisation will be higher, while the principle of privacy by design needs to be better articulated. In addition, according to Article 36, authorisation from the supervisory authority prior to the processing of personal data is mandatory if there are indications of high risks, in order to ensure the compliance of the intended processing with this regulation and in particular to mitigate the risks involved for the data subjects.

Directive (EU) 2016/680, which is focused on the protection of personal data that are being used for the police and criminal sector, shall better protect citizen's data, when processed for any law enforcement purpose including prevention of crime. It will protect everyone, regardless of whether they are a victim, criminal or witness. All law enforcement processing in the Union must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Supervision is ensured by independent national data protection authorities, and effective judicial remedies must be provided.

The directive describes those individuals who are subject to the capturing and processing of their personal data as 'data subjects' and further defines them as 'an identified or identifiable natural person'. In the context of personal data related to a data subject it says the following: ' "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'.

This broad definition means that surveillance systems in public spaces, where any category of data subject can be expected, will be subject to extra scrutiny, as also innocent citizens not under suspicion will become data subjects. That implies that the system must comply with a variety of rights of the data subjects and obligations for the operator/controller who need to respect those rights. These rights and obligations are related to the purpose for the collection and processing of the data, the period for which the data will be stored, the right to request from the controller access to and rectification, erasure or restriction of processing of the personal data concerning the data subject, and various additional obligations that serve transparency and accountability. The directive also describes the right of the data subject to obtain from the controller confirmation as to whether or not personal data relating to them are being processed.

The Article 29 working party ([13]) has also done work on the legal aspects of biometrics. Still based on the privacy and data protection regulation from 1995, the group adopted an opinion on the development of biometrics ([14]) in 2012. In general the opinion says that biometric technologies are closely linked to certain characteristics of an individual and some of them can be used to reveal sensitive data. In addition many of them allow for automated tracking, tracing or profiling of persons. Therefore their potential impact on the privacy and the right to data protection of individuals is high. This impact is increasing through the growing deployment of these technologies, e.g. in CCTV systems and smartphones. The opinion further assesses the legality of the collection of photographs on the internet for secondary purposes:

([13]) http://ec.europa.eu/justice/data-protection/article-29
([14]) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

‘Photographs on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose.’

This opinion clearly limits the collection and use of the existing photographs on the internet and in fact suggests that the earlier-mentioned mass collection of facial images by the NSA might be challenged for its legality and might prove to be illegal, when put to the test against applicable law. Based on this opinion it seems obvious that for capturing faces through CCTV systems in public spaces, similar restrictions are applicable. The group further discusses the use of biometrics for identification, meaning that the biometric information of an individual is used to establish identity or to verify a claimed identity. It is evident that the data must be accurate at enrolment and when the link between the person and the biometric data is being established. If identification is used through CCTV systems and biometrics, certain minimum levels of quality are required in order to prevent mistakes (the wrong person is identified) or complete failure (person could not be identified due to low quality). Unfortunately there is no standard way of expressing quality of the biometric data for these systems, meaning that safeguards against mistakes caused by low quality of biometric data should be found in the manual adjudication of the comparison results.

Further, the opinion refers to Article 15 of the Directive 95/46/EC regarding the automated processing of personal data, including biometrics, saying:

‘Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.’

When projected to CCTV systems using facial recognition that means that there is always the need for a human intervention and decision in order to take impactful decisions based on the recognition of a face. Regarding the storage of the biometric data the opinion states that central storage increases both the risk of the use of biometric data as a key to interconnect multiple databases (which might lead to creating detailed profiles of an individual) as well as the specific dangers of the reuse of such data for incompatible purposes especially in the case of unauthorised access. As CCTV systems are typically based on a centralised architecture we can apply this risk to those systems.

The opinion mostly follows the content and structure of the Data Protection Directive 95/46/EC, while adding some examples for practical clarification. One of the general risks the group sees in the context of new developments of biometric technologies is the possibility of covert collection, storage and processing as well as the collection of material with highly sensitive information that can invade the most intimate space of an individual. This covert collection is a major threat to the privacy and the power of individuals to control their private data.

3.5. Data protection by design and by default

An important aspect of the new regulation is the introduction of the concept of ‘data protection by design (DPbD) ([15]) (also known as ‘privacy by design’). This concept should guarantee that data

[15] Article 25 of Regulation (EU) 2016/679.

protection safeguards are built into products and services from the earliest stage of development (data protection by design). Privacy-friendly techniques such as pseudonymisation are encouraged, to reap the benefits of big data innovation while protecting privacy. However, what exactly is meant by DPbD is not specified in detail. This will leave room for discussion and interpretation, which will make it hard to use DPbD in a formal way. For that data protection commissioners may offer guidance and codes of conduct in the future. The Article 29 working party (see also the previous paragraph) has attempted to provide some definition to privacy by design, by attributing formal 'development life cycles' to the development of new technologies and applications. This development life cycle consists of the following steps:

- Specification of requirements based on a risk analysis and/or a dedicated privacy impact assessment (PIA);
- Description and justification on how the design fulfils the requirements;
- Validation with functional and security tests;
- Verification of compliance of the final design with the regulatory framework.

This approach can be applied for DPbD. It takes DPbD as a process, which needs to be followed in order to achieve deployments that are compliant with the principle of DPbD. The regulation further states that the implementation of appropriate measures is done by default. If a standard is to be considered as a default design, a set of optional data protection measures should be built into this standard in order to make the standard comply with European legislation.

As important changes in the design can occur during the development process, these steps of the development lifecycle may need to be repeated each time such changes are made. Standardisation can also be considered as development process, where consensus needs to be achieved on the design and specifications. Standards define functionalities, technical specifications, architectures, etc. The development of standards such as the draft VSS standard ISO 30137-1 therefore needs to integrate the privacy aspects into the overall design and to show clearly how privacy-protecting measures can optionally be built into the design, depending on the applicable legal requirements.

3.6. Biometrics and CCTV

CCTV (closed circuit television) applications are undergoing great advancements in capabilities. Miniaturisation of high quality cameras, fast processing of data and IP-based camera networks allow for complex and versatile surveillance systems. Recent developments are that biometrics such as facial recognition are being integrated into the CCTV systems.

The parallel ERNCIP Thematic Group Video Surveillance for the Security of Critical Infrastructures ([16]) has made an overview of use cases. The overview below contains use cases (partly derived from the above mentioned overview) where biometrics can be involved.

- Public order management
    - Checking watch lists (including faces in the crowd)
    - Identify, follow suspects (including multiple cameras)
    - Pre crime: identify suspected criminal real time (during offence)
    - After crime: identify suspected criminal off line (after offence)

([16]) https://erncip-project.jrc.ec.europa.eu/networks/tgs/video

    - Measuring crowd density
- Public transport
    - Checking watch lists
    - Connect owner to luggage
    - Left luggage: determining owner, detecting owner, following owner
- Private building/area access control
    - Access control of employers
    - Detect, follow and identify trespassers/intruders (including multiple cameras)
- Crisis management
    - Victims identification
    - Identification of relatives
    - Identification of terrorist and other criminals
- Public buildings
    - Checking watch lists (including faces in the crowd)
    - Identify, follow suspects (including multiple cameras)
    - Pre crime: identify suspected criminal real time (during offence)
    - After crime: identify suspected criminal off line (after offence)

The above overview is just a brief list of use cases for biometrics and CCTV. A more in-depth study is warranted to expand this list, while more elaborated specifics about the exact purpose and functionalities of the biometric technology should be added. The way biometric technologies and methods are to be used does have a significant impact on the technical design and specifications. That includes technical and procedural measures to protect the privacy of the data subjects. So it may be desirable that a standard such as the draft ISO 30137-1 shows the potential connections between the main functional variables and the consequences these may have on the privacy and data protection requirements for the envisaged biometric functionality. For European deployments it will be necessary to assess such an international standard on conformity with EU legislation. So far it seems that such assessment has not been done yet as it concerns an international standard. Therefore it would be advised that that privacy and data protection issues are monitored and possibly addressed.

This brief overview above already shows how diverse the applications are: positive vs negative identification, private vs public spaces, real time vs off line analysis, controlled vs uncontrolled environments, single faces vs crowd etc. These various use cases ask for a standard that is capable of being applied to a number of areas within the scope of the standard. The draft VSS standard ISO 30137-1 aims for the kind of usages as described in the above overview.

4. Findings and conclusions

The previous paragraphs briefly indicate the complexity of using biometric technologies for large-scale systems that involve a variety of data subjects. Video surveillance has been used as an example and referenced various times, mainly because the use of (facial) biometrics seems a logical step in the further development of those systems. However, more generally, surveillance seems to be of specific concern because of the likely large-scale use of biometrics in the future for this type of application and the potential for covert use. In this era of national and international threats to the security of our society, collecting as much data as possible is becoming an overall trend. Biometrics are of particular interest as they can identify individuals both in the physical world (e.g. border control, on the street) and in the cyber world (Google, Picasa, etc.).

Governments and private companies are collecting information about citizens on a large scale. Private companies often do so, based on mechanisms of consent that are not transparent. That makes it difficult for citizens to know which data are being collected and which parties are sharing this information and for what purpose. These practices therefore may need to be assessed by national and European data protection authorities to check their compliancy with EU and national legislation. This is already happening, as we can see in the ongoing cases against companies such as Facebook, WhatsApp and Google.

It is intriguing to see that privacy of individuals is under extreme pressure and that citizens are increasingly living in 'glass houses' under almost permanent monitoring through their smartphones and computers, while at the same time we have new privacy and data protection legislation that provide more and better means to protect privacy. Theoretically this is a logical development, but in practice this may be difficult as this legislation needs to be implemented uniformly in order to ensure that it makes a difference. Also we have seen that in the development of international standards privacy and data protection are not a standard component of the development process, as is shown by the draft ISO standard 30137-1 for the use of biometrics in surveillance applications.

We conclude that biometrics is becoming an increasingly important and effective tool to increase security, in certain cases providing convenience (e.g. automated border control and mobile payments). However, the pressure to give up privacy may turn against our freedom with a yet unknown impact. The current business model of citizens being a product rather than the client has unethical aspects considering that citizens are not fully informed about the price they pay and who benefits from their data.

With regard to the protection of critical infrastructures biometrics, CCTV and other surveillance systems are major tools to identify criminals and to deter crime. Cyber surveillance certainly needs to be taken into account as an area for further investigation, as biometrics are being used increasingly in cyber space. In addition, transparent biometrics (i.e. biometric methods that don't need active involvement of the data subject) can be a serious challenge due to the potential for covert capturing and usage. The increasing pressure of keeping our critical infrastructures and our society as a whole safe and secure, should not lead to underestimating the importance of keeping the used technologies, solutions and applications sufficiently transparent in order to ensure that the balance between privacy and security remains as we may expect in a free and democratic society.

5. Recommendations

The recommendations have been divided between those of more general nature and those that concern the next stage of the work of the ERNCIP TG Biometrics.

5.1. General recommendations

To ensure the proper and beneficial use of biometrics for surveillance and large-scale public and private applications the following general recommendations are made:

1. European standards for applications using biometrics need to take into account the latest European legislation. International standards need to be assessed on their compliancy to European legislation.

2. A privacy and data protection impact assessment following the concept of data protection by design and by default needs to be applied in the formal 'development life cycle' of applications and standards.
3. The combined use of CCTV and biometrics pose specific risks for privacy and therefore requires legal protection, while the developments in technology and deployment should be closely monitored and assessed by national and European DPAs.

4. National DPAs of EU Member States must be given the legal and financial powers to execute their regulative function. Specific capabilities need to be developed regarding biometrics. Further, coordinated guidelines and action by these DPAs are required with regard to obligations to deliver data protection impact assessments, prior consultation and appropriate safeguards.

5. Specific attention needs to be paid to the purpose limitation of captured biometric data, measures to restrict function creep, transparency of installation and operation of surveillance systems using biometric recognition and exercise of the legitimate rights of the data subjects.

6. More specific guidance and codes of practice based on the European regulation on the use of biometrics by governments and private parties needs to be developed.

5.2. Recommendations for future work of the Biometrics thematic group

1. An effort should be undertaken to define requirements and potential solutions regarding privacy preserving storage of biometric data.

2. Executing specific research in the area of biometrics and cyber surveillance regarding state-of-the-art technologies and societal impact.

3. Initiation of pre-normalisation standards activity in order to develop specific complementary standards and guidelines for surveillance systems using biometrics, in order to comply with specific EU regulations on privacy and data protection. This will involve working with the relevant CEN working group(s).

4. To set out the possible next steps for EU policy areas regarding the use of biometrics in cyber surveillance and CCTV.

LB-NA-28389-EN-N

JRC mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy directorates-general, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/986068

ISBN 978-92-79-64822-9