INTERNATIONAL STANDARD

ISO/IEC 24714

First edition
2023-07

Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance

Biométrie — Aspects transjuridictionnels et sociétaux de la biométrie — Partie 1: Recommandations générales

Reference number
ISO/IEC 24714:2023(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

This first edition of ISO/IEC 24714 cancels and replaces ISO/IEC TR 24714-1:2008, which has been technically revised.

The main changes are as follows:

— addition of privacy by design and privacy by default principles;

— addition of examples.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document provides support for the further development of ISO/IEC biometric International Standards in the context of cross-jurisdictional and societal applications of biometrics, including standardization of both existing and future technologies.

Specifically, this document offers guidance on the design of systems that use biometric technologies to capture, process and record biometric information:

— with regard to societal norms and legal requirements of jurisdictional domains (within and among various levels of jurisdictions);

— pertaining to privacy/data protection of an identifiable individual;

— with respect to an individual's ability to access and use these systems and the information they contain;

— with regard to health and safety issues pertaining to an individual when systems are utilized to capture biometric data.

In this document, biometric data are considered to be personally identifiable information (PII).

Examples of the benefits to be gained by following the recommendations and guidelines in this document are:

— enhanced acceptance of systems using biometrics by subjects;

— improved public perception and understanding of well-designed systems;

— smoother introduction and operation of these systems;

— potential long-term cost reduction (whole life costs);

— increased awareness of the range of accessibility-related issues;

— adoption of commonly approved good privacy practice.

The primary stakeholders are identified as:

— operators – those who use the results of the biometric data,;

— developers of technical standards;

— subjects – those who provide a sample of their biometric data;

— writers of system specifications, system architects and IT designers;

— public policy makers.

Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance

1 Scope

This document gives general guidance for the stages in the life cycle of a system's biometric and associated elements. This covers the following:

— the capture and design of initial requirements, including legal frameworks;

— development and deployment;

— operations, including enrolment and subsequent usage;

— interrelationships with other systems;

— related data storage and security of data;

— data updates and maintenance;

— training and awareness;

— system evaluation and audit;

— controlled system expiration.

The areas addressed are limited to the design and implementation of biometric technologies with respect to the following:

— legal and societal constraints on the use of biometric data;

— accessibility for the widest population;

— health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information.

This document is intended for planners, implementers and system operators of biometric applications.

Specification and assessment of government policy are not within the scope of this document. However, this document is intended to be beneficial to public authorities when deploying biometric systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
accessibility
extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of user needs, characteristics and capabilities to achieve identified goals in identified contexts of use

Note 1 to entry: Context of use includes direct use or use supported by assistive technologies.

[SOURCE: ISO 9241-112:2017, 3.15[1]]

3.2
data subject
subject
individual whose individualized biometric data is within the biometric system

Note 1 to entry: The data subject is the data principal of PII.

[SOURCE: ISO/IEC 2382-37:2022, 37.07.05, modified — The original term "biometric data subject" has been changed to "data subject" and Note 1 to entry has been replaced.]

3.3
function creep
expansion of a project, mission, or system's function beyond its original goals

Note 1 to entry: Function creep is the result of the intended or unintended change or extension to the functions of a system, which occur as small incremental stages, and can lead to significant changes to the function.

3.4
proportionality
balance between the interests of an individual and the interests of an organisation

3.5
usability
extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

Note 1 to entry: The "specified" users, goals and context of use refer to the particular combination of users, goals and context of use for which usability is being considered.

Note 2 to entry: The word "usability" is also used as a qualifier to refer to the design knowledge, competencies, activities and design attributes that contribute to usability, such as usability expertise, usability professional, usability engineering, usability method, usability evaluation, usability heuristic.

[SOURCE: ISO 9241-11:2018, 3.1.1[2]]

3.6
personally identifiable information
PII
any information that a) can be used to identify the PII principal to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

Note 2 to entry: In this document the PII principal is the data subject.

[SOURCE: ISO/IEC 29100:2011, 2.9[3].]

4 Symbols and abbreviated terms

API	application programming interface
DPIA	data protection impact assessment
DPO	data protection officer
FRR	false reject rate
FAR	false accept rate
GDPR	general data protection regulation
HTTP	hypertext transfer protocol
ICT	information and communication technology
IT	information technology
PET	privacy enhancing technology
PIN	personal identification number
REST	representational state transfer NOTE REST is an architectural style that defines a set of constraints and properties based on HTTP.
UCD	user-centred design
UI	user interface

5 Cross-jurisdictional and societal considerations

5.1 General

This document provides generic recommendations that are not specific to technologies or applications and that can affect all biometrics.

This clause begins by providing principles, guidelines and considerations for the design and implementation of biometric applications in three major areas:

1) cross-jurisdictional issues related to privacy and protection of personal information (see 5.2);

2) accessibility (see 5.3); and

3) an examination of health and safety issues when using biometric applications that can affect design and implementation considerations (see 5.4).

It considers usability and highlights conditions of the physical environment that can affect the operation and usability of a biometric application (see 5.5), societal, cultural and ethical aspects of biometrics (see 5.6) and acceptance of the use of biometric applications (see 5.7).

Two use cases are provided in Annex A as practical illustrations.

5.2 Cross-jurisdictional issues

5.2.1 General

The developer of a biometric application should take into account a number of issues that relate to specific jurisdictional requirements, which can differ between jurisdictions, not all of which are within the scope of this document. The list of issues which have not been examined in detail in this document includes:

— anti-discriminatory laws;

— disclosure laws;

— redress mechanisms;

— contractual issues;

— provision of biometric data to parties other than the data holder;

— provisions for law enforcement agencies for access to biometric and associated information;

— opt-in and opt-out rights and associated requirements for fall-back processes;

— specific data retention conditions (including period of time and security standards);

— evidentiary requirements for use of biometric data in a court of law;

— specific instances where biometrics are required by organizations or governments (e.g. for secure access to military facilities and critical infrastructure);

— applicability of legal domains in use of biometrics on the internet;

— border control laws.

5.2.2 Privacy aspects of biometric applications

With the proliferation of biometric applications worldwide, the aspect of privacy gains importance. As a result, it is necessary to understand what the objectives of data protection law and policy intend. It is necessary that the applicable law and policy protect data subjects and their biometric data and personal rights. Using a biometric application means using PII; thus, existing privacy laws apply. Depending on how a system is deployed, biometric technology can compromise or protect a data subject's privacy. The possibility of protection is especially valid in view of the special properties of biometrics, which are linked uniquely to the subject for their lifetime, unlike PINs and passwords, which are indirectly and weakly linked to a person. By using a biometric key, other types of PII can be better protected from theft and misuse than by traditional means. Biometrics can therefore be both an object and a tool in the different aspects of this discussion. In all applications, the principle of proportionality should be applied. That means that biometric data used should be adequate, relevant and non-excessive with regard to the purposes for which they are collected and further processed.

Biometrics can be considered in the context of PETs. PETs are a coherent system of ICT measures that protect privacy by eliminating or reducing PII or by preventing unauthorised, unnecessary and/or undesired processing of PII; all without losing the functionality of the data system.

NOTE 1 Processing in this context includes any operation or set of operations which is performed upon PII, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

The principle of PET applies to biometrics seen from two standpoints:

— as an object of the principle, the implementation and application of biometrics should follow a comprehensive and correct privacy regime in order to be privacy enhancing;

— as a tool in the meaning of PET, biometrics itself can be a privacy enhancing method.

For instance, biometrics can improve the verification process compared with a traditional process where a subject has to provide information through requested evidentiary documents which can reveal considerable personal information. The use of biometrics can simply be putting a fingerprint on a sensor without revealing any additional personal information (name, address, date of birth, etc.) to the person who is checking the entitlement of the identified person (given that there has been a proper registration process beforehand). Moreover, the use of biometrics enables the subject to bind a device (such as a smart phone) to their identity. The advantage is that, although a device can have more than one user, the biometrics bind the use to a single specific identity. Subjects can use pseudo-identities by varying the biometrics provided.

The following are some generally accepted rules of PETs.

— At the planning stage, assess whether or not biometrics should be used or another less intrusive method substituted

— Use no PII or as little as necessary.

— Use encryption if using PII.

— Destroy raw data as soon as possible.

— Anonymize PII wherever possible.

— Do not use central databases where not required.

— Give subjects control over their PII.

— Use a means of evaluation and certification to verify that an application delivers a guarantee of an appropriate level of trust.

NOTE 2 See also ISO/IEC 24745[4].

In relation to privacy, Article 17 of the International Covenant on Civil and Political Rights[14] stresses that no one's privacy, family, home or correspondence should be subjected to arbitrary or unlawful interference, nor should their honour and reputation be unlawfully attacked.

Privacy is one of the most significant issues confronting not only the biometrics industry, but also any organization which gathers personal information. The potential for shared access to information and multiple uses of biometric databases raises specific concerns. However, many statements on privacy fail to capture the nuances across various biometric deployments. Certain types of biometrics engender a greater perception of privacy invasion while others have little influence on privacy concerns. PII is the first step to establishing personal identity and it is at this point where many crimes of identity occur. Although there are many issues associated with submitting biometric data, it should be reinforced that identification will have already been established through other identity documents such as birth certificates. Therefore, many people might consider biometric techniques to be far less invasive than being asked, sometimes face to face, questions relating to their personal history, details of residence and information about other members of their family, such as a mother's maiden name. In this context, biometric technology is simply another means for identification.

The increasing number of implementations and discussions about the use of biometrics raises questions about the technology's impact on privacy in applications generally available and widely used by the public, in the workplace and at home. Key aspects of privacy issues relate to either the data subject or the organization. From the data subject's perspective, issues relate to collection, choice, use and security of information and anonymity of the individual. From an organizational perspective, issues include the manner and purpose of collection, solicitation, storage and security of information, access to records, relevance and the limits on use and disclosure of collected data.

Other privacy issues relate to concerns that include stigmatization and reputational or financial damage. An example of stigmatization in some communities has been the association of fingerprints with criminal activity. However, fingerprinting is now also becoming associated with the more positive

identification of the law-abiding citizen as a holder of electronic ID documents, a cardholder, or club member. Any concerns can be exacerbated by the possibility that a person's biometric can be "spoofed".

Further privacy issues relate to function creep, or the misuse of information, and tracking or aggregation of data. In relation to function creep, using data for a secondary purpose can appear worthwhile; however, socio-cultural and legal issues can arise when individuals are not informed of this secondary purpose for which their information will be used, and have not given consent for this to take place. "Tracking" can refer to a specific form of function creep where biometric data is used in combination with additional data such as spending or travel details to track the actions of individuals. Covert use of biometrics without legal authorization will impinge on individuals' privacy.

In addition to the analysis of cross-jurisdictional issues relating to privacy listed in 5.2.3, a number of other considerations should be taken account of, including:

— issues relating to the linking of biometric data to other information;

— transition states, e.g. the ability to give consent changes:

  — migration from a minority to a majority age,

  — change in mental capacity (e.g. Alzheimer's disease),

  — death of a subject,

  — revocation procedures;

— notification to anonymously enrolled data subjects of any changes in the uses of a biometric.

The system data protection officer, or equivalent, should take part in the planning and implementation of all biometric applications. They should also drive the development and implementation of the biometric privacy policy and ensure conformance to that policy. Where there is no data protection officer, there should be a person in charge of implementing the system who is able to deal with IT security and privacy issues when they occur.

If recognized national consumer associations have published recommendations on biometrics that seem to be applicable to a specific biometric implementation, a system operator should consider them where appropriate.

5.2.3 Privacy principles for biometric applications

There are a number of key privacy-enhancing principles that should be considered by organizations implementing a biometric application. These principles, which are listed below, build upon the reference documents listed in the Bibliography. They should be considered and applied in the context of jurisdictional laws and regulations.

1) Transparency

   There should be a general policy of openness about the use of biometric data, which should include the purposes for which the data is to be used and the point of contact responsible for its use. Any subsequent changes should be made known to data subjects.

2) Consent

   Biometric data should be collected, stored, used, disclosed and retained with the knowledge and consent of data subject, except where local laws have exemptions to this principle.

3) Preference for opt-in

   Where feasible and practical, opt-out or opt-in procedures should be made available to the data subject. In general, opt-in is the preferred option.

4) Limitation of purpose

The purpose(s) of a biometric application should be available for data subjects to read prior to their use of it. The biometric data processing should be limited to the stated purpose.

NOTE In some countries the principle of necessity is used. This requires that for use of a particular methodology or technology, especially emerging technology, it be demonstrated that its use is required and that the purpose cannot be achieved by any other methodology and/or technology that is accepted as providing adequate protection of individuals privacy.

5) Limitation of collection

The collection of biometric data should be limited to the minimum required to achieve the stated purpose(s).

6) Limitation of period of retention

The biometric data should be kept only for the period of time necessary for the specified purposes. Procedures should be specified for secure removal of data that is beyond its retention period.

7) Adherence to performance criteria

The system operator should ensure the correct configuration, function and stability of a biometric application according to its specification. This is so that system operation, or any system malfunction, does not result in unauthorized access, use, modification and disclosure of biometric data.

8) Access rights of the data subject

The data subject should be given reasonable access to verify the correctness of the biometric data and to have incorrect data amended.

9) Protection of the data

Biometric applications should be designed so that biometric data, including in back-ups or archive, is protected against unauthorized access, use, modification, deletion, disclosure and retention.

10) Secure audit

The biometric application should be designed to permit a secure audit of the use of biometric data including its deletion or removal from the biometric application (see ISO/IEC 27002[5]).

11) Data transfer between jurisdictions

The system operator should take reasonable steps to ensure that biometric data that is disclosed to an external party, including in another jurisdiction, is adequately protected. This may be done through contractual arrangements or a Memorandum of Understanding. Model contracts for the transfer of personal data can be used even though this might not be a legal requirement in the jurisdictions in which the external party operates.

12) Significant automated decisions

Where biometric applications are used to make significant and fully automated decisions about individuals, a mechanism to request the intervention of a person should be provided. Individuals should be notified of such automated decisions.

13) Accountability

A person within the system operator's organization should be accountable for conformance with the relevant law and these principles.

14) Accuracy of biometric data

Biometric information should be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

15) Anonymization of data

Release of biometric data for academic, statistical or testing purposes should be considered and controlled carefully. Links to other personal information should be removed where they could lead to identification of an individual.

16) Privacy by design

Organizations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing biometric data PII.

17) Privacy by default

When a system or service includes choices for the individual on how much PII they share with others, the default settings should be the most privacy-friendly ones.

5.2.4 Further legal aspects

5.2.4.1 General

Although this document is not intended to deal in detail with legal issues such as contractual or evidentiary aspects, some general statements on legal value and potential consequences of using biometric applications can be of benefit for its readers.

In some countries, a number of regulations exist that apply to the operation of biometric applications and the management of biometric data. Subclause 5.2.4 gives an overview of legal considerations, other than those related to privacy. Examples of detailed regulations applicable in specific countries are reported in the Bibliography.

5.2.4.2 Biometrics in authentication infrastructures

There is a need to facilitate electronic transactions between parties and, to achieve this, many countries have introduced electronic transaction regulations.

While hand-written signatures are widely accepted in the legal context, this normally relies on human signature recognition. For electronic transaction scenarios biometric data can be used on its own or in combination with a PIN or a password. When multiple factors are used in combination, this is referred to as multi-factor authentication.

Three-factor authentication can involve something that a subject possesses, something they are or something they know in any combination. Two factors are sufficient for most commercial applications. In this context, biometrics characteristics in combination with security token or credential can be seen as the equivalence of a hand-written signature. If the use of biometrics can realize the traditional functions of the hand-written signature, a legal transaction and the binding of it to a person can be ensured and therefore a similar legal binding force can be achieved.

Where both the captured and reference biometric data samples are needed to realize equivalent legal validity in transactions to that of a traditional hand-written signature, this requires that, in all cases, both systems employed are able to deliver strong security and a reliable audit trail (see ISO/IEC 27002[5]).

The use of biometric characteristics alone in electronic transactions can be deemed by some authorities not to confer the same legal validity as a hand-written signature. In these cases, biometric characteristics and digital signatures should be in a complementary relationship. Therefore, in this context, the use

of biometric characteristics needs to be considered as one module in a public key infrastructure and subject to the legal requirements of that infrastructure.

5.2.4.3 Biometric methods and legal proof

The evidential value of an electronic transaction can be maximized if one or more biometric credentials are used to prevent unauthorized issue of a legal declaration.

An appropriate level of security can enhance the evidential integrity: of the binding of the digital signature to the individual, and in the non-repudiation of the document or transaction.

Any legal challenges will best be addressed by demonstrating the reliability of the system which was used. Although the assessment of the court will differ between jurisdictions, the performance and the overall security of the biometric application will be the most significant aspect in the case.

It should be considered that recognition of a biometric data sample rarely performs perfect matching of characteristics in practical applications. It is therefore difficult to make reliable statements on the recognition quality of a specific system at a defined point in time. This contrasts with a PIN or a password where the match is one hundred percent true or false, but presents the risk that it can have been used by one who is not entitled to use it.

A system secured by biometric credentials is subject to similar security breaches as a system protected by PINs or passwords. Naive faith in technology can result in a higher degree of confidence in a biometric application's security than is justified. It is therefore essential to determine the degree of security in the total system (see ISO/IEC 27002[5]).

5.2.4.4 Performance of biometric applications and liability

Biometric applications are subject not only to technical malfunction but also to reduced performance as a result of user behaviour (including operators and subjects), deliberate or accidental, or as a result of aged biometric data samples. The failure to protect and secure biometric data can incur legal liability. It is important to consider the consequences and liability issues associated with such failures in the legal context.

NOTE ISO/IEC 21472[6] deals with user interaction influence in biometric application performance.

5.2.4.5 Standard terms of business

Liability can be dealt with in statutory provisions and also in contracts. Businesses often use pre-worded contract terms that, as a rule, add to the statutory provisions. In many countries, there are existing laws of standard terms of business, containing rules for whether such terms have become part of a contract, whether clauses are invalid, and entitle third parties (such as consumer associations) in certain circumstances to file a court claim aimed at obtaining a judgement holding a clause invalid. Generally, what is often needed, is a clear and understandable wording; in other words, the subject should be able to find and familiarize themselves with certain mandatory information, without difficulty.

It is desirable to establish consumer-friendly terms in order to build trust in a biometric application. Subjects are unlikely to use a biometric application for their convenience if they are disadvantaged by having the legal burden of proving whether or how they used the system in the event of a disputed match.

For instance, if the risk of malfunction of the biometric application prevents the subject's access to the protected area, standard terms of business should not shift the responsibility to the subject.

An exclusion of liability for system malfunctions following data subject interaction is also usually not permitted, or at least not desirable, in terms and conditions of business. Biometric applications are vulnerable to unauthorized use and malfunctions. Besides intentional manipulations by attacks on the system and general technical problems, a certain number of potential erroneous acceptances are always

to be expected to occur. The subject is neither able to affect nor to control these technical aspects since these aspects are in the operator's sphere alone.

5.2.4.6 Non-discrimination

Since biometric systems use physical or behavioural information, individuals can be deterred from using them if they are unable to present the required characteristic or cannot do so in such a manner as to achieve successful verification. Examples are represented by missing fingers, inability to speak, inability to control eye movement. Considering the increasing use of biometrics, this is likely to become a problem for affected subjects especially when biometrics are required to access important services.

In many countries, legislation exists to minimize direct or indirect discrimination with regard to, for example, disability, sex, age and ethnicity. Biometric systems should be designed so that the differential impacts (see ISO/IEC TR 22116[7]) are minimized. To avoid discrimination against individuals who are unable or do not consent to use a particular biometric application, provisions should be made for alternative methods of identity verification that are similarly secure and usable as the biometric method.

5.2.4.7 Biometrics in the workplace

In several countries, specific regulations need to be taken into account when biometric technology is used for physical or logical access control in a working environment. The workplace requires special consideration since the employee's ability to refuse consent is constrained by their dependence on employment. In order to protect the rights of the employees, in particular with regard to their privacy, it often makes sense to involve a workers' association, a works council, or equivalent, in order to negotiate sensible use and management of the biometric data. When employment ceases or in a job application that requires a biometric data sample to be submitted, the biometric data should be deleted as soon as possible.

5.2.4.8 Aspects of criminal law

5.2.4.8.1 Altering data and unauthorized computer access

Under many criminal laws there is a prohibition of altering electronic data without authorization and it is also not legal to access a computer of another person without appropriate entitlement. The specific cases under which legal sanctions are applicable depend on the national regulations.

5.2.4.8.2 Forgery or theft of biometric data

A spoofing attack on a system by copying or theft of biometric characteristics can be subject to criminal law in various jurisdictions. There can be a need to establish specific regulations in this regard in order to protect the wellbeing and life of subjects. Technical measures are being developed to ensure that the biometric data is not tampered with, by testing the liveness of biometric characteristics, for example. Systems should therefore provide such a test, a verification that the biometric data sample is provided by a natural person, and include measures against "replay" or re-presentation of a sample. These features can mitigate subjects' concerns over theft of physical biometric characteristics and should be implemented where possible.

The ISO/IEC 30107[8] series on biometric presentation attack detection establishes a framework through which presentation attack events can be specified and detected so that they can be categorized, detailed and communicated for subsequent biometric system decision-making and performance assessment activities. It also establishes data formats to be used and principles and methods for performance assessment of presentation attack detection algorithms or mechanisms.

5.3 Accessibility

5.3.1 General

A biometric application should be easily accessible to all subjects and should not disadvantage any subject. Accessibility of a biometric application is dependent on specifics of the subjects using the system and on its usability, including the physical environment (see 5.5.2). For subjects that cannot use the biometric application due to permanent or temporary conditions, alternative systems are necessary and should be provided. Any additional costs to the subject that are associated with the use of biometric applications should be clearly stated.

Accessible systems should be designed to be:

— equitable in use for data subjects;

— inclusive in operation for data subjects who have physical or psychological inabilities;

— flexible in use;

— simple and intuitive to use;

— easy-to-understand with appropriate additional prompts;

— clearly indicated by signs;

— tolerant of error;

— usable with low physical effort;

— of a size and in a space that allows easy approach and use;

— using a range of tactile, audio and visual prompts in the user interface.

Accessibility difficulties can be long term, temporary and/or can occur without warning, for example, as the consequence of sudden onset of illness such as laryngitis or a sore throat, dental or eye surgery, or other physical injuries.

Subject groups can be internal or external to the implementing organization or can be a combination of both. It is imperative that any organization contemplating the introduction of biometrics identifies all stakeholders, considers how the subject groups might respond to the technology and identifies potential issues and solutions prior to programme implementation. Human factor issues are not confined to those who are the subjects of the technology but can also include system implementers, designers, technicians and biometric attendants, who can all be subject to system limitations and errors.

Reasonable efforts need to be made to support accessibility based on analysing costs and benefits to reduce the number of exceptions that need to be handled and to reduce the impact on other users (operators and subjects).

Many countries have adopted inclusive policies and enforced them with legislation (e.g. the USA's Americans with Disabilities Act of 1990[15]). ISO/IEC Guide 71[9] gives an overview on the possible impairments of subjects and helps to address their problems when standardizing and/or implementing systems. The United Nations Standard Rules on Equal Opportunity for Persons with Disabilities[16] provides guidelines on the enhancement of participation opportunities for people with disabilities in education, employment, social security, culture, recreation, transport and accessibility to the built environment and information. In Japan, the domestic standard (JIS X8341[17]) with regard to accessibility, was published in May 2004. Access to biometric technologies is described in JIS X8341.

The system operator and/or designer should take into account the following disabilities and problems for subjects using a system. Some of these conditions can be temporary. Note also that many people have a combination of impairments, the cumulative effect of which can amplify the impact of individual impairments.

Examples of disabilities:

1) The absence of physical body parts required for the correct operation of a biometric or its specific instantiation in the system.

   EXAMPLE 1 Missing index finger(s) in an access control system using prescribed fingers.

2) The absence of behavioural features required for the correct operation of a biometric or its specific instantiation in the system.

   EXAMPLE 2 Data subject with no power of speech required to use a voice-activated door entry system.

3) Unusable physical body parts required for the correct operation of a biometric or its specific instantiation in the system.

   EXAMPLE 3 Person with extreme arthritis asked to use a flat plane hand geometry biometric.

4) Unusable behavioural features required for the correct operation of a biometric or its specific instantiation in the system.

   EXAMPLE 4 Data subject in a country with a writing system based on non-Latin alphabet required to use a dynamic signature system designed for Latin alphabets,

5) An inability to present the required biometric characteristic in a sufficiently consistent and predictable manner under the particular conditions of operation.

   EXAMPLE 5 Uncontrollable movement of the eyeball resulting in difficulty in operating an iris recognition system.

   EXAMPLE 6 Person with a speech impediment (e.g. stuttering) asked to use a speaker verification scheme.

6) An accelerated drift, that is a change in a characteristic over a period of time in physical or behavioural aspects resulting in increasing difficulty in meeting the matching criteria for an identification or verification.

   EXAMPLE 7 Data subject with conditions that rapidly age the facial features being verified in certain automatic face verification systems.

7) An inability to access, or difficulty with physical access to, the biometric sensor or user terminal.

   EXAMPLE 8 Data subject using a wheelchair or person with a stature not tall enough to access a sensor or user terminal fixed at a specific height.

8) An inability either to read, due to illiteracy, or to understand the instructions, or to recall the correct procedures, in order to operate the biometric application successfully.

   EXAMPLE 9 Forgetting which finger was enrolled in an unattended access control system, and being locked out after three attempts.

9) Psychological conditions that prevent the data subject operating the biometric applications correctly.

   EXAMPLE 10 Persons with extreme compulsive-obsessive disorder required to use sensors or keypads/keyboards with physical contact.

10) Conditions, such as those listed above, which result in disproportionate use of resources.

    EXAMPLE 11 Senior citizens who require a longer period of adjustment to changes in context and situation, exceeding the notional time allowed for an authentication.

11) Inability to capture biometric information for children or individuals that do not have “standard” size biometrics.

    EXAMPLE 12 Child using a hand geometry reader due to the position or size of the sensor.

In addition to those who are not able to use the system, there are occasions when a data subject can want to opt out of the use of the biometric and the system operator and/or designer can wish to consider granting this as an option. This option can affect the benefits of the use and the functionality of this method of authentication.

In some cases, the problems can be mitigated by changes in the design of the environment (e.g. by providing height-adjustable sensors or optimized lighting conditions). In other instances, alternative designs should be considered.

The approach to the design of accessible biometric applications (as well as other alternative, non-biometric approaches) will be dependent on a number of factors, including:

— whether or not the use of the system is voluntary or mandatory;

— the consequences of an adverse outcome, failure to recognize, to the subject (e.g. personal safety, financial impact, social exclusion or embarrassment, or effect on quality of life);

— the likely demographics of the target data subject group.

Designers should aim for the best overall performance for the maximum number of potential subjects, and creative and innovative design should be encouraged. The sharing of knowledge and experience of best practice should in due course lead to consistency in presentation and use of biometric applications.

5.3.2 Principles for less able subjects

In order that potential data subjects with less ability should not be disadvantaged in the application of systems using biometrics, care should be taken to design these systems to operate in accordance with the following accessibility principles:

1) Inclusive design

   Biometric applications should be designed so that as many subjects within the target population as is reasonably possible can use the system effectively and with the minimum of discomfort. Information messages can be provided in more than one form, such as visual and audible.

2) Early consideration of the needs of people with less ability

   In the design of such new systems or services, the needs of less able subjects should be considered from the outset.

3) Testing

   Before systems are deployed, they should be thoroughly tested by subjects who represent the widest range of abilities (that is, in respect of visual, auditory, physical, cognitive and behavioural ability).

4) Training

   For less able subjects, training appropriate to enable the use of the system for the widest range of abilities should be offered.

5) Choice

   Wherever practicable, the subject should have a choice of biometric applications to use and should not be disadvantaged if their range of ability prevents them from using a specific type of biometric characteristics.

6) Alternative method

   Where no alternative biometric technology is available and the range of ability prevents the use of the particular biometric technology, subjects should be permitted to use an alternative method.

Wherever practicable, the use of such an alternative should not result in an inferior level of service or functionality to the subject.

7) Re-enrolment

If the subject can no longer reliably use a verification system, the subject should be provided, wherever feasible, with the opportunity to repeat the enrolment process.

8) Staff training

Staff who operate systems that use a biometric technology should be trained in how to work with less abled people.

9) Consent

A biometric application should not store details of a subject's range of abilities without his or her informed consent.

10) Equality

The rights of a subject across all ranges of abilities should be the same.

5.4 Health and safety

5.4.1 General

The lack of information and awareness by the public of biometric technologies and their applications has generated discussion on health and safety issues. As biometric technologies become more widespread in organizations, fears that some people can already have about the use of these methods can be exacerbated by misinformation in the mass media. At an individual level, performance can be affected by these fears and perceptions, which can minimize the useful benefits of these technologies to society. To some extent, even willingness to use biometric devices can be dependent on the extent of perceived intrusiveness of the technologies in relation to health and safety issues.

In particular, there are two specific concerns when considering health and safety issues in the application of biometric technologies:

1) The direct medical implication of the use of biometric technologies, i.e. the potential risk for the body associated with the use of the technologies. Examples of direct medical implications are:

   — physical contact with the sensing device, leading to possible infections,

   — illumination by visible or invisible light, and any potential consequent damage to a sensitive organ.

   If subjects express such health and safety concerns, these concerns usually do not reflect the reality of using these devices. Indeed, many fears are not based on any scientific foundations. Nevertheless, because of these concerns, the successful implementation of biometric applications often requires that subjects be informed of any possible risk that can result from use of the device.

2) Indirect medical implications reflect privacy concerns occasioned by possible disclosure of a health condition during a biometric process. This means data which are not needed for the actual biometric process but, under some specific circumstances or with additional processing or analysis, can give information about an extraordinary state of the subject.

   Subjects can be concerned that medical information derived from such data could affect their life insurance and employment situation, particularly if biometric information is shared or accessed between organizations.

5.4.2 Addressing the health and safety issues

To the extent that there are real threats to health and safety, the designer and system operator of the biometric application should consider the following issues.

— Biometric devices should conform to health and safety standards, where applicable, and reference these standards. Subjects should be informed of any potential health and safety implications.

— In specific environments where contagions or harmful substances are present, precautions should be taken to reduce the risk of cross-contamination to acceptable levels.

5.4.3 Special cases

There can be people who experience particular psychological or physical sensitivity in the use of a particular method. While these are not easy to anticipate, system operators should be aware of the effect of such sensitivities on the performance of biometric applications. System operators should be prepared to provide accommodation where possible.

Consideration should also be given to specific environments such as hospitals, where for example medical staff cannot use fingerprint systems due to the requirement for scrupulous hand hygiene. Other examples include abattoirs, food service or manufacturing industries, pharmaceutical industries and border control and quarantine organizations where contact can be made with non-health assessed individuals. The requirement to wear protective clothing for occupational, health and safety or climatic reasons can also affect the integration of biometric technologies inducing the use of touchless technologies.

5.5 Usability

5.5.1 General

Usability of a biometric application is key to optimal performance. This is equally valid for mandatory and voluntary biometric applications.

In 5.5.2, some aspects regarding the usability of biometric applications are presented. This list is not exhaustive. Moreover, for each of the possible biometric methods, specific usability issues need to be considered.

The effect of these factors varies considerably according to the specific biometric technology being used and the application in which it is deployed.

Aging of a subject can impact the performance of verification when comparing with an unchanged biometric reference. The data subjects' capability to use the biometric application can also degrade with age.

5.5.2 Usability and the context of use

5.5.2.1 General

The success of biometric applications is dependent on the physical environment in which they operate. Problems can be created by extremes of climate, contamination from dust or chemicals, the need for protective clothing and exposure to vandalism, levels of artificial or natural illumination, the position and orientation of the biometric device and the presence of other fixtures and fittings in the vicinity. The level of verification rates is dependent upon the quality of the enrolled biometric sample which requires ideal conditions for its enrolment. In practice, in non-ideal verification conditions better verification rates can be achieved, if the enrolment requirements follow the guidance in ISO/IEC TR 29196[10]. Different environmental parameters are important for different biometric modes.

The physical environment in which biometrics operate has an effect on the performance and usability of biometric applications. For example, there should be clear instructions, documentation for subjects and reassurance on the use of data and the health and safety aspects of the technology.

NOTE The ISO/IEC 24779[11] series on pictograms, icons and symbols for use with biometric systems specifies a family of icons and symbols used in association with devices for biometric enrolment, verification and/or identification.

5.5.2.2 Climate

Climate can present problems to sensitive biometric devices if they are subject to extreme environmental conditions such as temperatures or humidity. In outdoor locations this could include exposure to fog, rain or snow and ice or condensation on a sensor such as a camera lens. Data subjects can have to remove gloves, hats, scarves or sunglasses. Extreme temperatures can cause the biometric data sample to be more dry or moist depending on the environment. High temperatures can cause the subject to sweat and can impede the capture of the biometric data. For example, a facial verification can be adversely affected by presence of sweat on the user's face. Extremely dry environments can prevent the optimal capture for fingerprints.

NOTE ISO/IEC 29197[12] addresses fundamental requirements for planning and execution of environmental performance evaluations for biometric systems based on scenario and operational test methodologies.

5.5.2.3 Contamination

Contamination from dust or chemicals can require unusually high maintenance activity to prevent corrosion of devices and to keep devices clean. This can occur in engineering or industrial locations or in locations where food is prepared and there are high levels of oil particles from food frying. In some environments a special enclosure for the device can be required.

Protective clothing can present problems for biometric devices when they take measurements, for example, hard hats, protective glasses, goggles and welders' masks, face masks that cover the mouth and nose, rubber or other protective gloves, and heavy boots or knee protectors that can modify a subject's posture.

5.5.2.4 External or public areas

Devices in external locations or internal public spaces can be subject to various challenges, such as vandalism, including attack with a heavy or sharp object or by spray-paint. High levels of ambient noise from people, machinery, public address systems or traffic can prevent voice biometrics from being collected or verified. These factors can also prevent users and subjects from hearing spoken instructions, which will be especially problematic for blind or partially sighted subjects who rely on these instructions.

In many public areas booths or kiosks should be provided in a controlled environment, so that the required verification levels can be achieved.

5.5.2.5 Location

Location of biometric devices is important where active participation by the subject is required. The place where the device is located should be clearly indicated by signs, which should ideally be illuminated and have smart-sign capability to alert blind and other people with less ability to their presence. Textured floors can also guide people with a visual impairment to the device.

For attended applications, the location of the biometric sensor should allow the actual biometric capture operation to be in full view of the biometric attendant.

The device location should also prevent background interference during the biometric capture but should allow assistance for children by adults or for less abled people by a caregiver.

Some applications present particular challenges in locating the biometric sensor. For example, a vehicle-based system where passengers in the car are required to verify their biometric data. Or, if only verifying the driver, the variance in height of the vehicle would have to be taken into account for facial recognition.

The selection of the appropriate biometric in locations where people with temporary injuries are using the biometric system (e.g. a hospital accident department) needs to be based on a detailed analysis of the nature and frequency of their injuries. This analysis is to be carried out before the design and procurement of the biometric application and should consider enrolment as well as verification.

5.5.2.6 Throughput and data subject population

Consideration should be given to peak throughput in a location, queue management, the number of biometric devices needed and the time required, and its variability, for successful enrolment and/or positive or negative verification. The nature of the data subject population should be considered when selecting an appropriate biometric for the system.

The use of contactless "on the move" biometric systems can be beneficial in environments where high throughput is desired.

NOTE See ISO/IEC TS 22604[13].

5.5.2.7 Position

The position and orientation of biometric devices is important and consistency between the enrolment and verification systems is, in most cases, an essential requirement. The devices should be accessible to the subject community and located in a consistent position. There should be guidance on the position in which the subject should stand or sit when using the device, and variations in the subject's height and reach should be accommodated. Ideally there should be some feedback to the subject on his or her correct orientation, placement or volume in the case of a voice-based system.

NOTE The ISO/IEC 24779[11] series on pictograms, icons and symbols for use with biometric systems specifies a family of icons and symbols used in association with devices for biometric enrolment, verification and/or identification.

5.5.2.8 Information and education

User guides should be available near public biometric devices. A helpline number or address should be displayed in a prominent position adjacent to the facility for use in the case of failure of the system or of the subject to use it successfully. Users in business or domestic environments should be trained to ensure they are familiar with the device before they approach it to perform essential tasks. The enrolment personnel should receive specific training to enrol subjects in an appropriate manner.

5.5.2.9 Ease of use

The user interface of a biometric device requiring active participation by the data subject should be intuitive. The sequence of actions should be logical if the data subject is required to present his or her biometric characteristics and is also required to present a token, e.g. a smartcard, or entering an identity or account number. This can need to be researched in order to ascertain data subject expectations and using appropriate standards. Instructions should be provided in visual and audible form, and graphical and/or visual or audible cues should prompt actions. The data subject may be required to take some action to indicate that he or she is in position and ready to present his or her biometric data. Feedback should indicate success or failure and prompt a retry where appropriate. In some environments it is possible to capture biometrics passively and without the subject having to actively participate in the capture process. For example, while the subject is reading the screen a facial biometric verification is being performed. The subject should be made aware that biometric verification takes place in this environment.

5.5.2.10 Support

Assistance should be provided especially where the operation of a biometric device is unattended and success is required for the data subject to progress. In the event of problems in presenting biometric data or with some other operation of the device, a help facility should be available to allow the subject to ask for assistance from a person either remotely or on site. Alternatively, the subject should be able to invoke other procedure, e.g. on a building access system this may be a doorbell or buzzer. In a domestic context the data subject needs to have access to an override procedure in the event of injury or an activity which prevents him or her from presenting biometric data. An override procedure should also be available for use in emergencies.

5.5.2.11 Further issues

In addition to these issues, levels of illumination, whether from artificial or natural light, can affect verification rates for some biometric techniques and the usability of a system. Vibration and motion of the system's operating environment should also be considered.

5.6 Societal, cultural and ethical aspects of biometrics

5.6.1 General

This subclause considers societal, cultural and ethical effects on biometric solutions taken together as a whole.

Social, cultural and ethical aspects that affect biometric applications are influenced by legislative, political, emotional and economic issues. Although the diversity of these aspects within and especially across jurisdictions is extremely great, the set of privacy principles given in 5.2.3 provides a minimum of generally agreed good practice.

The technical limitations of any particular biometric technology should not lead to discrimination against any particular ethnic or social group.

In addition to topics already discussed in the previous subclauses of this document, the following should be considered.

5.6.2 Commonalities and diversities

While some cultural, social and ethical aspects can be common among cultures, there are also differences which can affect biometric applications. For example, most cultures currently accept photographic evidence of identity and therefore can accept biometric face recognition. In contrast, individuals in some cultures can have strong objections to touching shared surfaces like fingerprint sensors or hand geometry units.

5.6.3 Multinational environments

When proposing a biometric application for a multinational user population, for example for a time and attendance application, metaphors and imagery appropriate for the respective cultural groups should be included in all information and training material.

5.6.4 Anonymity

The desire for anonymity varies among individuals in different cultural and application contexts and therefore biometric applications should be configured to offer flexibility in the degree of anonymity provided. For example, some biometric applications do not necessarily need to know the personal details of a subject. They can only need to verify entitlement or prevent multiple enrolments.

5.6.5 Clothes, ornaments and traditions

In some cultures, the individuals can be reluctant to use biometric technologies as they believe that these seriously compromise their cultural, social and ethical practices or beliefs.

For example, a biometric application that relies on facial recognition can be in disharmony with a culture in which the normative behaviour is to wear a veil or head scarves. A biometric application that is negatively influenced by cultural or socially related body ornamentation (e.g. make-up, tattoos, jewellery, clothing or facial hair) might not be practical or highly acceptable.

5.6.6 Compulsory participation

Some biometric applications can require compulsory participation. The extent to which this is acceptable can depend on cultural and social demographics. For example, enrolling in and using a biometric application can be a prerequisite to obtaining employment or entering a secure location.

In summary, the issues surrounding cultural, social and ethical aspects of biometrics are complex, and vary both in content and across national boundaries. It is incumbent on those responsible for biometric programs to be sensitive to such distinctions. Awareness and careful consideration of the cultural, social and ethical aspects of biometrics are therefore prerequisites for all phases of biometric application implementations.

5.7 Acceptance

5.7.1 General

A crucial aspect for the success of biometric implementations is acceptance of the systems by the subjects who are to use them. As biometric uses increase, it will be important to assess the public's evolving view on the technology, its applications and its observance of privacy protection. If individuals do not accept the system, observations of projects and real world applications indicate that the overall performance will be poor. This does not depend on whether the use of the system is mandatory or voluntary. Even within a compulsory system, individuals can reject the system with non-cooperative behaviour that, over time, is likely to result in a substantial decrease in recognition rates. Therefore, it is crucial to be aware of the factors which determine acceptance, this includes positive and negative aspects. It is necessary to know how acceptance can be increased and which factors lead to less acceptance by subjects. The interaction between a user and a biometric application can only work successfully where it results in efficient and effective completion of the desired task. This interaction takes place in a particular context which includes not only a physical and organisational but also a cultural environment. This context affects the interaction and vice versa.

Concerns can be categorized as logically-founded or deep-seated subjective concerns. Many people with a technical background will be comfortable with the first group, but might not realize the need to address the less tangible aspects.

Literature and project surveys describe a number of factors which can have an impact on the acceptance of a biometric application or application:

— privacy/data protection;

— convenience;

— reliability and performance;

— consumer-friendly legal conditions;

— ease-of-use;

— cost-performance-ratio;

— life-cycle;

— invasiveness;

— health and hygiene;

— sex;

— religion, ethic and culture.

The maximum acceptance can be achieved if the biometric application is of the greatest tangible benefit for the subject. On the contrary, if the subject does not see any benefit by using the system, the willingness to use it and thus the overall acceptance of the application will decrease substantially. Moreover, the less tangible the benefit for the subject, the less willing he or she will be to accept potential risks caused by the use of the biometric application.

In general, for biometric applications to be successful it is desirable that they reduce physical and mental workload on subjects. Whilst biometrics have an inherent advantage over knowledge-based mechanisms, this advantage can only be realised if certain preconditions are met. Moreover, it has to be considered that the use of a physical characteristic is viewed as more intimate and personal than a PIN or a password. Fear and shame can cause negative reaction to the system, and there is a need of non-discriminating use (e.g. individuals who are not able to use the system need to have a back-up and must be protected against negative gossip e.g. at the workplace). To be rejected from a biometric application can embarrass the subject, especially if this happens repeatedly and if this causes delay to other people, and thus reduces acceptance of the system or the technology in general.

In addition to the acceptance factors listed above, other success factors that have been identified include:

— that a biometric application provides a good fit to the production and security tasks that subjects have to carry out, i.e. integrated into the work process;

— that a biometric application performs well (high speed, low error rates) at all stages of use (installation, registration, daily use, contingency);

— that a biometric application is trusted to be safe, keeping the biometric data securely and not using them for other purposes.

Transparency of the overall system for the subject is another crucial success factor. Positive attitude towards biometrics can therefore be increased by higher visibility of biometric technologies in the media. The more the individual knows about the system and its details, advantages and risks, the more they can develop trust. Previous work on multimedia applications suggests that risks to subjects need to be made explicit upfront, and users are given a choice to accept them. This applies to privacy risks (e.g. function creep), health and hygiene aspects and issues of reliability and performance. Furthermore, trust in the user or operator of a system, of any type, is frequently a factor in the subject's trust in the system itself.

Positive attitudes towards biometrics correlate with simplicity, speed and convenience over a longer period of time. For details, see 5.5.

There are a number of trade-offs to be made, for example, between an apparent reduction in personal privacy and a perception of increased security. Certain groups will position this trade-off at different points, and the prospective implementer and operator of a biometric application should consider the various groups within the user community.

Examples of the way in which such groups can be approached are:

— age;

— gender;

— education;

— occupation;

— expertise;

— culture;

— ethnicity;

— 'caring' responsibilities, e.g. parents of school age children, and people responsible for the elderly and vulnerable;

— socio-economic grouping and origin;

— attitude to authority and previous involvement with the police.

Across the different cultures all over the world there can be significant differences in the attitude towards biometrics and different levels of information. Cultural differences might even be stronger than gender or age differences. There can be differences in the privacy assessment as well as in the rating of performance and security.

5.7.2 Privacy and acceptance

Privacy safeguards (or rules) seem to be critical acceptance factors for individuals who are to use biometrics. The majority of individuals who were interviewed were in favour of biometrics (e.g. in order to combat identity theft), but at the same time are concerned about possible misuse of their personal information. On the other hand, there are trade-offs that people are willing to make between privacy and convenience. The success of point-of-sale, pay-by-touch systems shows that, for many people in many contexts, convenience is more important than privacy. This does not mean that privacy concerns can be ignored in such systems, and implementers should strive to provide both privacy and convenience.

Experiences indicated the greatest possible transparency is able to reduce privacy fears. This should include information in advance of the use and the reason for the use as well as information about how the biometric data are used, shared, and in which manner they are processed. People's concerns also seem to include the possible combination with other personal identifiers and the risk of tracking people's movement. Another trust factor is the ability of the individual to check that biometric data is correct.

A comprehensive security concept should require that biometric data that are used are considered as PII and mechanisms to secure those data are provided.

5.7.3 Reliability, performance and acceptance

Where there is a lack of confidence in the accuracy and reliability of biometric technology (e.g. high throughput times, high rates of false rejection and poor user interfaces), this can result in reduced acceptance. For some social groups and cultures, fear is a normal psychological response to the unknown. High false rejection rates can lead to decreased acceptance, although this seems to depend on the applications purpose. Whereas in high security areas individuals are likely to accept more attempts to get identified, in more convenience driven applications they are probably not ready to accept more than three attempts. This also depends on the information subjects are given in advance of the implementation and use.

5.7.4 Recommended actions for acceptance testing

Operators should consider the following factors as a minimum:

NOTE This is not a comprehensive checklist.

1) Piloting of the biometric application should be undertaken, and the acceptance factors determined for all groups which will be potential subjects of the biometric application.

2) Check the user population for the specific application in order to address the concrete concerns of the respective subjects.

3) Planners should remember that although systems may be designed initially for early adopters and/or specific target groups, subsequent extension to other groups of subjects may require additional testing and redesign.

4) Specific aspects related to biometrics include the need for re-enrolment as people age.

5) One way to improve user acceptance can be to adjust the threshold in a biometric application in order to reduce the rate of false rejections. However, this carries a corresponding penalty of a reduction in security. The relation between false acceptance and false rejections should be explained to the subjects.

6) Provide information and usage guidelines understandable for non-technical persons and, dependent on the user population, in different languages.

7) If acceptance testing is undertaken, the subject group should be allowed to familiarise themselves with the biometric application in the context of the application.

8) Both education and marketing of the intended use of the biometric is crucial to address both the logically sound concerns and subjective cultural uncertainties.

9) Check that the target environmental conditions (such as temperatures or humidity) won't affect the false rejection rate.

10) Check the health precautions engaged regarding the risk of cross-contamination.

Annex A
(informative)

Examples for consideration of cross-jurisdictional and societal aspects in biometric applications

A.1 SpeechXRays

A.1.1 Project description

SpeechXRays is a research funded project. It belongs to the H2020 work programme under number 653586[18].

The goal of the SpeechXRays project is access control, both for logical access (e.g. to web sites or databases) or physical access (e.g. to a restricted place of a critical infrastructure). SpeechXRays uses two types of biometric characteristics for access control: face recognition and speaker recognition. Because these two types of biometric characteristics can be easily acquired with common IT devices (laptop, smartphone), they can be used by almost anyone with basic IT equipment, from anywhere, without dedicated biometric devices, for both enrolment and verification. Face and voice can be stolen easily too, therefore SpeechXRays focuses especially on security and fight against spoofing or other illegitimate use of a stolen identity.

A.1.2 Considerations regarding privacy

System design has involved the study of three realistic use-cases, representing the most likely usage of the SpeechXRays project outcome. In the context of testing the use cases, privacy was addressed by three independent testing entities.

All three use-case implementations involved the consultation of the data protection officer (DPO) of the entity implementing the use case, and the consultation the ethical committee of the entity. For one of these use-cases, a meeting with the national data protection Authority took place. This use case relates to the usage of SpeechXRays in a “workforce scenario” (i.e. physical and logical access control within a professional entity). IFIN-HH, a Romanian research Institute in nuclear physics, was in charge of implementing this use case in its premises. During the meeting between the Romanian Data Protection Authority (in Romanian: Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal – A.N.S.P.D.C.P.) and IFIN-HH, some measures of the DPIA were discussed. A letter notified IFIN-HH that the test was approved, and security conditions were specified, mostly related to physical security measures on hard disks and computers on which the test platform had to be implemented.

All three testing entities decided to have accuracy and acceptability measured on a standalone platform, implemented on a personal computer, with no smartphone of tablet clients. However, the security measures to protect PII selected for the test were finally different according to the testing entities:

— One entity selected to erase all user data (except log that have no PII) after a maximum of 3 days. This is very safe as the disk is really overwritten (hard to rebuild), but this limits the extent for the FAR measurement test.

— Another entity selected, for its employees (but not for visitors and students) to write the user data on an external encrypted hard drive, keep the hard drive in a safe until the end of the test, and do the full FAR measurement test at the end of the test.

— The third entity selected to have dedicated computers, permanently kept under employees supervision, where the data will be kept until the end of the test to perform full FAR measurement test

In all cases, the user data is fully erased at the end of the test.

A.1.3 Considerations regarding other cross-jurisdictional issues

As mentioned in A.1.2, all three use-case implementations involved the DPO, and the ethical committee of the testing entities when available.

In the context of the test, consent forms were written, and signed by the testers. Their main shared characteristics was that:

— They explained the purpose of the project and the purpose of the test

— They reminded the end users of their rights (according to GDPR)[19]:

  — Right to be informed

  — Right to data rectification

  — Right to data erasure

  — Right to restrict the data processing

  — Right to data portability

  — Right to object

  — Right not to be subjected to automated decision-making

— They mentioned that there was no risk to use the SpeechXRays test platform.

— They mentioned the PII retention period

— They mentioned that no compensation will be given

— They mentioned the effort that was expected in term of time spent

— They mentioned a contact point (e-mail, telephone) for enquiries

The main ethical guidelines that were followed during SpeechXRays test are listed below:

— Participation in the testing process of the SpeechXRays platform was exclusively voluntary, as each user of the system had to agree with the recording and subsequent processing of his/her biometric data (i.e., voice and facial expression recordings).

— Participating or not participating has no impact on potential users (i.e. if they are students or employees).

— Participation in the testing process of the SpeechXRays platform did not waive any legal rights or released any of the members of the SpeechXRays consortium from liability for negligence or fraudulent use of biometric data.

— All users of the SpeechXRays platform have been informed in detail about the scientific goals of the SpeechXRays project, the role of testing that was carried out in the testing entities, as well as the security of the biometric data during the testing period and its subsequent deletion.

— The users involved in the testing process of the SpeechXRays platform had the right to ask that their biometric data was deleted at any moment during the testing period without giving reasons or being penalized for withdrawing from the testing process.

— The final statistical results of the SpeechXRays testing process will be published such that it is impossible to determine the individual users that were involved.