TECHNICAL REPORT

ISO/IEC TR 24714-1

First edition
2008-12-15

Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications —

Part 1: General guidance

Technologies de l'information — Biométrie — Considérations juridictionnelles et sociétales pour applications commerciales — Partie 1: Guidage général

Reference number
ISO/IEC TR 24714-1:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 24714-1, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC TR 24714 consists of the following parts, under the general title *Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications*:

— *Part 1: General guidance*

The following parts are under preparation:

— *Part 2: Specific technologies and practical applications*

Introduction

This part of ISO/IEC TR 24714 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 part of ISO/IEC TR 24714 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 part of ISO/IEC TR 24714, biometric data are considered to be personal data.

The contents of this part of ISO/IEC TR 24714 are recommended practices and guidelines. They are not mandatory. Legal requirements of the respective countries take precedence and biometric data should be obtained in accordance with local norms of behaviour. This part of ISO/IEC TR 24714 does not reduce any rights or obligations provided by applicable laws. Compliance with any recommendations in this part of ISO/IEC TR 24714 does not of itself confer immunity from legal obligations.

Examples of the benefits to be gained by following the recommendations and guidelines in this part of ISO/IEC TR 24714 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

— users – 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.

Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications —

Part 1: General guidance

1 Scope

This part of ISO/IEC TR 24714 gives guidelines 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.

The intended audiences for this part of ISO/IEC TR 24714 are planners, implementers and system operators of biometric systems.

Specification and assessment of government policy are not within the scope of this part of ISO/IEC TR 24714.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
accessibility
〈biometrics〉 possibility for everyone, regardless of physical capability or technological readiness, such as people with disabilities, to access and use biometric technologies and services

NOTE 1 Access can be gained directly, using assistive technologies or by the use of alternative methods. One should strive to enable direct access by as many subjects as possible (inclusive design).

NOTE 2 The ISO/IEC JTC 1 Special Working Group on Accessibility defines accessibility as “the usability of a product, service, environment or facility by people with the widest range of capabilities”.

2.2
attendant
individual who is present to guide or assist a (data) subject in enrolling or verifying their biometric data

2.3
(data) subject
individual who provides biometric data for storage or comparison in a biometric system

2.4
function creep
mission creep
expansion of a project, mission, or system’s function beyond its original goals

NOTE 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.

2.5
biometric data manager
person within the system operator’s organization accountable for compliance with the principles contained in this part of ISO/IEC TR 24714

2.6
proportionality
balance between the interests of an individual and the interests of an organisation

2.7
spoofing
〈biometric system〉 presenting a recorded image or other biometric data sample, or an artificially derived biometric characteristic, in order to impersonate an individual

2.8
usability
extent to which a product can be used by specified users (subjects) to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

NOTE Adapted from ISO 9241-11:1998, 3.1.

2.9
personal data
information relating to an identified or identifiable individual that is recorded in any form, including electronically or on paper

2.10
jurisdictional domain
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of external constraints on people, their behaviour and the making of commitments between people including any aspect of a business transaction

NOTE Adapted from ISO/IEC 15944-5:2008, 3.67.

2.11
biometric data sample
data captured from a biometric sensor that can be recorded as a biometric reference for a subject or used for comparison with previously recorded biometric reference data to verify or identify a subject

3 Symbols and abbreviated terms

PET Privacy Enhancing Technology

ICT Information and Communication Technology

PDA Personal Digital Assistant

4 Societal and cross-jurisdictional considerations

4.1 Introduction

This part of ISO/IEC TR 24714 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 systems in three major areas: jurisdictional issues related to privacy and protection of personal information (4.2); accessibility (4.3); and an examination of health and safety issues when using biometric systems that may affect design and implementation considerations (4.4).

It continues with a discussion of usability addressing “real world” issues surrounding biometrics. It considers usability and highlights conditions of the physical environment that may affect the operation and usability of a biometric system (4.5).and continues with the societal, cultural and ethical aspects of biometrics (4.6); and discusses acceptance of the use of biometric characteristics (4.7).

4.2 Jurisdictional issues

4.2.1 General

The developer of a biometric system needs to take account of a number of issues that relate to specific jurisdictional requirements, which may differ between jurisdictions. Although some of these are considered in this part of ISO/IEC TR 24714, a number of others will not be examined. The list of issues which have not been examined in detail in this part of ISO/IEC TR 24714 includes

— anti-discriminatory laws,

— disclosure laws,

— redress mechanisms,

— contractual issues,

— provision of biometric data to other companies or subsidiaries,

— 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 national infrastructure),

— applicability of legal domains in use of biometrics on the Internet,

— border control laws.

4.2.2 Privacy

With proliferation of biometric systems 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 to protect not only processed data but also to protect data subjects themselves and of their personal rights. Using a biometric system means using personal data; 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 only indirectly and weakly linked to a person. By using a biometric key, other types of personal data 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 Privacy Enhancing Technologies (PETs). PETs are a coherent system of Information and Communication Technologies (ICT) measures that protect privacy by eliminating or reducing personal data or by preventing unauthorised, unnecessary and/or undesired processing[1)] of personal data; all without losing the functionality of the data system (see Borking/Raab 2001).

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

— as an object of the principle, the implementation and application of biometrics has to 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 the subject has to give full information of his/her person along with revealing all personal information on the requested document. The use of biometrics can simply be putting a fingerprint on a sensor without revealing any additional personal information (name, address, birth date 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 PDA) to their identity. The advantage is that the protected device cannot be used by other persons. Subjects can use pseudo-identities by varying the biometrics provided.

---

1) Processing in this context includes any operation or set of operations which is performed upon personal data, 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 following are some general accepted rules of Privacy Enhancing Technologies.

— Use no personal data or as little as necessary.

— Use encryption if using personal data.

— Destroy raw data as soon as possible.

— Anonymize personal data wherever possible.

— Do not use central databases where not required.

— Give subjects control over their personal data.

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

In relation to privacy, Article 17 of the *International Covenant on Civil and Political Rights* [36] states:

> "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".

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 may have little influence on privacy concerns. Personal information 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, a myriad of 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 is 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 cardholder, club member and consumer. 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 may appear worthwhile; however, socio-cultural and legal issues may 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 section 4.2.3, a number of other considerations may need to 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 data protection officer of the system operator, or equivalent, should take part in the planning and implementation of all biometric technologies and applications and should also be included in the establishing and compliance control of the biometric privacy policy. When there is no internal 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.

When 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.

4.2.3 Privacy principles for biometric systems

In certain applications biometrics allow a measure of privacy to individuals through verifying their identity rather than identifying them. They may also contribute to the enhancement of privacy in other systems by controlling access to sensitive data.

In order to protect the privacy of individuals, certain measures should be considered by organizations implementing a biometric solution.

This list builds upon the reference documents listed in Annex A, providing the user of this part of ISO/IEC TR 24714 with a minimum of commonly agreed good practice. Nevertheless, appropriate legal authorities should be consulted in order to ensure compliance with all local laws and regulations, since – in some countries – some of these principles will be mandatory and have specific obligations attached to system operators using biometric applications.

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, 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 subject. In general, opt-in is the preferred option.