Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

30-Jun-2004

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2003)2/FINAL
Unclassified

**Cancels & replaces the same document of 28 April 2004**

## Working Party on Information Security and Privacy

# BIOMETRIC-BASED TECHNOLOGIES

www.oecd.org/sti/security-privacy

JT00166988



English - Or. English

## FOREWORD

This report is intended to provide an understanding of the benefits and limitations of biometric-based technologies. It also includes information on existing privacy and security methodologies for assessing biometrics.

The report was prepared, with comments from member countries, by Peter Hope-Tindall, a consultant to the OECD, under the supervision of the secretariat. Peter Hope-Tindall is the Director and Chief Privacy Architect of dataPrivacy partners.

This report was declassified by the Committee for Information, Computer and Communications Policy on at its 46th Session on 1-2 April 2004. It is published on the responsibility of the Secretary-General of the OECD.

**TABLE OF CONTENTS**

## EXECUTIVE SUMMARY

This report provides a general introduction to biometric technologies. It also discusses the various concerns raised by these technologies, with a focus on privacy and information security.

There is currently considerable interest and activity associated with the use of biometrics in many different areas such as banking, education and other public services as well as in the travel security context. Further, biometric-based technologies hold the opportunity to identify individuals in remote network environments and through varied modalities of communications. Also, the biometric industry has experienced substantial growth in the recent past and is expected to experience even more growth in the next five years. A number of biometric standards have been or are being developed to support the industry and the technology. World events and the search for a technological solution to the security problems that many have identified have increased the interest in biometric-based technologies and the biometric industry in general.

The world of biometric-based technologies brings with it new terms and concepts, an understanding of which is important to an informed discussion of the subject matter. The report introduces the following major biometric-based technologies: finger-scanning, hand geometry, facial recognition, iris scanning, retinal scanning, finger geometry, voice recognition and dynamic signature verification. A brief description of other, more obscure biometric-based technologies such as ear geometry, body odour measurement, keystroke dynamics and gait recognition is also provided. DNA-based technology, which is not strictly a biometric, but raises many of the same concerns as biometrics, is addressed in Annex III.

All biometric systems operate in essentially the same manner. They capture a biometric sample, perform feature extraction or dataset creation and perform one of two types of searches. They provide either a one-to-one (1:1) or a one-to-many (1:N) search capability. As regards the biometric system performance, the reader is cautioned as to the lack of independent, publicly available performance reports and the importance of context in the consideration of any performance statistics. However, a number of metrics are useful in the discussion and comparison of biometric-based technologies and may provide some sense of objectivity in the choice of specific technologies. Among the metrics discussed are: false reject rate, false acceptance rate, equal error rate, failure to acquire and failure to enrol. Additional factors such as throughput, cost, ease of use, user acceptance and transparency, while not primary indicators of biometric system performance, are key to the success of any implementation. The report discusses issues related to the performance of biometric-based technologies along with their appropriateness for certain applications. A high-level summary is presented together with a number of examples of existing and planned applications.

The report also discusses a number of concerns related to biometric-based technologies in particular in relation to security and privacy. Three primary areas of privacy concern relate to *i)* the potential of 'function creep' in biometric systems; *ii)* the risk that these systems may become an infrastructure of surveillance; and *iii)* that consent and transparency may be optional in certain biometric implementations. As regards security, the report points to the recent discussion surrounding the weaknesses of biometric systems. A number of specific attacks (spoofing, tampering, replay attacks, etc.) must be anticipated and protected against in a biometric system.

To address these privacy and security concerns, the report proposes that system designers utilise biometrics as an appropriate solution to a security problem and architect appropriate backup and exception processing procedures into the overall system design.

A number of techniques are discussed for implementing privacy and security into a biometric system: statutory methods (legislation as a tool of biometric system design), policy methods (policy development and incorporation into biometric systems) and the use of technology, such as tamper-proof hardware to proscribe and govern biometric system operation. Additional formal techniques such as privacy architecture and security architecture are also introduced. These aim at ensuring that the raw elements of privacy and security are constructed into systems as raw materials. In this respect the report recommends that the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* be embodied in any biometric system design and project.

The report also discusses other shared concerns about biometric technologies such as the risks of inappropriately trusting a biometric system as a sole security measure, the lack of independent, publicly available biometric performance reports, and the risks of implementation of biometric-based technologies as a panacea.

Finally, the report makes the case for the encouragement of a multi-national initiative to enhance research, development and education related to biometrics. Such initiatives should embrace the OECD guidelines by incorporating both privacy and security instead of forcing us to choose.

# BIOMETRIC-BASED TECHNOLOGIES

## Background and context

### *Purpose of this report*

The report has been prepared to provide an introductory understanding of biometric-based technologies together with a discussion of the strengths, weaknesses and capabilities of the respective technologies.

It is hoped that with discussion, appropriate methodologies may be identified or developed to facilitate the privacy-enhancing and security-enhancing implementation and deployment of biometric-based technologies.

Readers are cautioned that conclusions and recommendations may not be applicable in all circumstances.

### *Privacy*

*What is privacy?*

Privacy has been described in various ways ranging simply from "the right to be left alone," (Warren and Brandeis, 1890)[1] to the right that individuals have to create and maintain a "personal space" around them in both physical space and cyberspace free from interference by others.

When we talk about our right to privacy, we usually mean the right to do the following within the bounds of the law:

- Keep our personal information to ourselves, or to choose with whom we share it.
- Remain anonymous or unidentified with respect to certain personal and public activities, if we choose. (These activities might include the exercise of public rights like freedom of assembly, or private choices like our spending habits or our manner of worship.)
- Live our lives without being under surveillance by others.
- Conduct private communications.
- Have physical privacy and personal space.
- To be left alone, both as consumers and as citizens.

*Components of privacy*

Ownership and control

Although not universally accepted, an increasingly popular position is that information belongs to the data subject to which it refers – maybe not the paper file it resides in or the computer it is stored on, but the information itself is truly theirs. Therefore, they have a right to determine who has access to it, to authorise what it is used for, and to be provided with a mechanism to review the data and bring about any necessary corrections.

Complex nature of privacy

A view of privacy based on the Common Criteria for Information Technology Security Evaluation ("Common Criteria"*)* uses three qualifiers to express privacy: *identity*, *linkability* and *observability*. It has been proposed by some (Adams *et al.*, 2002) that these three domains may be used to describe privacy as a "three-dimensional figure" and may also be used to measure the relative "privacy" of a given system or technology (Hope-Tindall, 2002a).

*OECD Privacy Guidelines*

In 1980, recognising the importance of the data privacy issue in international commerce, the Organisation for Economic Co-operation and Development (OECD) issued the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("Privacy Guidelines") (OECD, 1980) that have become an important foundation for privacy since that time. The Privacy Guidelines were proposed to harmonise national privacy legislation and, while upholding human rights, prevent interruptions in international flows of data. They represent a consensus on basic principles which may be built into legislation, or serve as a basis for a self-regulation regime in those countries which have not adopted formal data privacy legislation. In Canada, the voluntary Canadian Standards Association (CSA) model privacy code,[2] based on the OECD Privacy Guidelines, has been incorporated as a schedule to the recently enacted federal privacy legislation.[3]

The OECD Privacy Guidelines formulate a set of eight principles, often referred to as Fair Information Practices.

The principles are (OECD, 1980):

**Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

**Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the Data Controller.

**Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

**Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

**Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

**Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle of the OECD Privacy Guidelines except:

- With the consent of the data subject.
- By the authority of law.

**Individual Participation Principle:** An individual should have the right:

- To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.
- To have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him.
- To be given reasons if a request made under this principle is denied, and to be able to challenge such denial.
- To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

**Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

### *Security*

*The role of security in protecting privacy*

"Too often, the debate is framed as if security and privacy are mutually exclusive" as stressed by Frank J. Cilluffo. "This is simply not true. It is wrong to think of the issue as 'either' 'or'. Stakeholders should rather think of the need to incorporate both. In order to preserve the twin goals of security and privacy, they must begin with the notion of a true partnership" (Cilluffo, 2000).

There is undoubtedly a need to strike an appropriate balance between privacy and security. Privacy and protection of personal data are important rights of fundamental value. Their respect is essential for the protection and promotion of human dignity. Nevertheless, compelling specifically identified public interests may justify limitations on privacy and confidentiality.

The principles of the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* ("Security Guidelines") (OECD, 2002) (for example, the Democracy Principle and the Ethics Principle) and those of the OECD Privacy Guidelines (for example, the Use Limitation Principle or the Security Safeguards Principle), aim at providing guidance to achieve compatible realisation of the goals of security of information systems and protection of personal data and privacy.

The fact that governments have the sovereign right to do what they must in vital areas such as national security and maintenance of public order is recognised in both the Security Guidelines and the Privacy Guidelines.

We suggest that with the appropriate design and policy decisions, we need not choose security or privacy over the other. Coherent solutions in the security area will have to take account of the broader economic and social issues.

*OECD Security Guidelines*

New Security Guidelines were adopted as a Recommendation of the OECD Council in late July 2002 (OECD, 2002).

Subtitled "*Towards a Culture of Security*", the Security Guidelines seek to recognise the growing reliance on information networks and the increasing number of threats against the security of those networks. They have already been commended by the US State Department as helping to mark a "new international understanding of the need to safeguard the information systems on which we increasingly depend for our way of life" (Williams, 2002).

Since their adoption in July 2002, the Security Guidelines have served as the basis for the United Nations General Assembly Resolution A/RES/57/239 for "Creation of a Global Culture of Cyber Security" in December 2002 and have been recognised by the Council of Ministers of the Asia-Pacific Economic Cooperation forum and by the Council of the European Union.

At the heart of these guidelines are nine guiding principles. The principles are (OECD, 2002):

**Awareness:** Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

**Responsibility:** All participants are responsible for the security of information systems and networks.

**Response:** Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

**Ethics:** Participants should respect the legitimate interests of others.

**Democracy:** The security of information systems and networks should be compatible with essential values of a democratic society.

**Risk assessment:** Participants should conduct risk assessments.

**Security design and implementation:** Participants should incorporate security as an essential element of information systems and networks.

**Security management:** Participants should adopt a comprehensive approach to security management.

**Reassessment:** Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

**Interest in biometric-based technologies**

Biometric-based technologies have recently received a great deal of interest as a possible solution to crime, terrorism and as a "foolproof" method of identification.

Whether or not these claims remain to be proven, it is becoming increasingly apparent that airports and border-crossing points will become the intense focus of biometric trials, deployments and study for the near future:

- In 2003, the European Union implemented biometrics across 14 member states to facilitate its refugee processing and asylum system (EC, 2003).[4]

- The head of the International Air Transport Association (IATA) has called for more stringent and expanded security measures for airports and airlines, including the use of biometrics (Chua, 2001).
- On 28 May 2003, The International Civil Aviation Organization (ICAO) adopted a global, harmonised blueprint for the integration of biometric identification information into passports and other machine readable travel documents (MRTDs). According to ICAO, "the increased use of biometric-enhanced MRTDs will lead to speedier passage of travellers through airport controls, heightened aviation security and added protection against identity theft" (ICAO, 2003a).
- In the United States, the Enhanced Border Security Act calls for the Immigration and Naturalization Service (INS) to take a unique biometric identifier, like a fingerprint or a face scan, from every alien entering and exiting the United States with a visa by 26 October 2004 (US House of Representatives, 2002). The United States is also extending the requirement for biometrics to be incorporated into tamper-resistant travel documents of other countries in its visa waiver programme as a condition of continued participation (Fonseca, 2002; US Department of State, 2002).

Biometric-based technologies are used today to restrict access to high-security facilities and information systems, to facilitate sign-on and authentication of online users.

As innovation and the search for convenience moves human interaction to non-traditional network-based delivery systems (such as automated teller machines [ATMs], smart kiosks, telephone or Internet-based banking, purchasing, voting, etc.), although the maturity of biometric-based technologies is by no means assured, they offer the potential to solve the one problem that seriously threatens these developments - specifically the ability to authenticate someone remotely.

Whatever our personal beliefs and preferences, the time has come for these technologies to be considered as solutions for the problems of today and tomorrow, for the advantages and disadvantages to be weighed with scientific certainty and for the security and privacy implications to be openly discussed.

## Biometric-based technologies

### *Definitions*

*Biometrics*

The term "*biometric*" is derived from the Greek words *bio* (life) and *metric* (the measure of).

> "Biometrics" has been defined as: "The automated use of physiological or behavioural characteristics to determine or verify identity." (IBG, n.d.a)
>
> *Although the term 'automated' is key to the definition of a biometric system, (for instance, a system of documents using pictures which are manually compared by a human being does not comprise a 'biometric' system).*
>
> *The reader is cautioned that the more appropriate term for this definition is perhaps, '**automated-assisted**' as in many cases the biometric system, due to its inherent statistical nature merely presents a 'degree of correlation' for a human to make a final decision regarding identity. (While some 1:1 verification systems may function in a largely automated manner [based upon an acceptance threshold and error rate set by the operator] – 1:N identification systems usually*

> *force the system designer to trade-off between having a human investigate a false acceptance [or rejection] and accepting an overall higher error rate.)*

Yet another definition makes it perfectly clear that this field of study refers only to human beings:

> "'Biometrics' are unique, measurable characteristics or traits of a human being for automatically recognising or verifying identity" (Roethenbaugh, 1998a).

The International Biometric Group (IBG), a well-known biometric testing and consulting company gives the following guidance for use of the various forms of the word (IBG, n.d.a):

> **Biometric:** (noun) – one of various technologies that utilise behavioural or physiological characteristics to determine or verify identity. "Finger-scanning is a commonly used biometric." Plural form also acceptable: "Retina-scan and iris-scan are eye-based biometrics."
>
> **Biometrics:** (noun) – Field relating to biometric identification. "What is the future of biometrics?"
>
> **Biometric:** (adjective) – Of or pertaining to technologies that utilise behavioural or physiological characteristics to determine or verify identity. "Do you plan to use biometric identification or older types of identification?"

*Biometric system*

The term "*biometric system*" may be defined as follows:

A ***biometric system*** includes all of the hardware, associated software, firmware and network components required to enable the end to end biometric enrolment and matching process.

*Is DNA a biometric?*

A commonly asked question, DNA-based technologies differ from standard biometric-based technologies in several ways:

- DNA requires an actual physical sample as opposed to an image, photograph or scan.
- DNA matching is not done in real time and, for the most part, is not automated.
- DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples.

In a strict sense then, DNA matching is ***not*** a biometric in the same way that traditional forensic fingerprint examination is ***not*** a biometric.

Regardless of these distinctions, we believe that DNA-based technologies should be discussed alongside other biometric-based technologies inasmuch as they make use of a physiological characteristic to verify or determine identity. Beyond the definition, to most observers DNA looks, acts and may be used like other biometrics. The policy ramifications, while much more serious for DNA-based technologies, share some common attributes with other biometrics.

Although not central to this report, a brief description and discussion of DNA-based technologies may be found in Annex III.

***Biometric privacy issues***

Biometrics, like all technologies, are defined by their usage. Biometric-based technologies, by their nature, are neither necessarily good, nor bad, for privacy. There are, however, a number of specific ***privacy concerns*** that apply to the use of this technology.

*Function creep*

"Function creep" (also known as "purpose creep") is the term used to describe the expansion of a process or system, where data collected for one specific purpose is subsequently used for another unintended or unauthorised purpose.

In privacy principle terms, we may think of function creep as a violation of the "finality" principles; the subsequent use, retention or disclosure of data without the consent of the individual and inconsistent with the purpose specification given at the time of data collection.

As an example, we may think of a social service (welfare) system that requires a finger scan to enrol. Let us assume that undertakings were made at enrolment to the user that the finger scan is being collected ***solely*** for the purposes of guarding against 'double dipping' (ensuring that the user is ***not*** already registered for welfare). If the finger scan were subsequently used for another purpose (*e.g.* something not described in the initial purpose specification) then we have 'function creep'.

*Infrastructure of surveillance/unique identifier*

An overarching concern for some people is that biometrics will become a technology of surveillance and social control. Perhaps as the ultimate personal identifier, they may be seen to facilitate all the ominous and dehumanising aspects of an information society – a society in which unparalleled amounts of personal information may be collected and used on a systematic basis. Encouraging this possibility, a risk exists that biometric authentication will become the default form of human identification and authentication, even in situations where a less intrusive method will suffice, merely because everybody has one (a biometric) and may already be using it. With a biometric identifier, the ease with which surveillance, through the use of data (or dataveillance), can be undertaken increases significantly. "Where all electronic transactions require biometric authentication, those who have access to transaction data also have a detailed portrait of the individual" (O'Connor, 1998). The inherent risk exists that biometric identifiers may be used to link transactional data without even the knowledge, never mind the consent of the data subject.

As noted by George Tomko, a privacy expert and designer of biometric systems, "Biometrics, if used as currently marketed by [most] biometric vendors – where the biometric template is used as the token of identification or verification – will further erode privacy and jeopardise our freedoms. The simple fact is that template-based biometrics are not privacy friendly. Any time you base verification or identification on comparison to a stored template you have a situation which, over time, will compromise privacy – either by business or government, in response to the next national emergency" (Tomko, 2002).

*Consent/transparency*

Certain biometrics may be used without the consent or active participation (or indeed even the knowledge) of the individual.

Facial recognition is already being used in casinos (Curran, 2001) to recognise cheaters and card-counters. In the United Kingdom, closed circuit television (CCTV) technology is being married to facial recognition technology to automate the recognition of criminals on city streets (Lack, 1999: Townsend and Harris, 2003). AC Neilsen, the market rating company, has patented a facial recognition system, which identifies shoppers to track their buying habits using facial recognition.[5] In each of these cases, the subject individual may be unaware that facial recognition is being performed.

Iris scanning can already be performed at a substantial distance (a range of 18 to 24 inches) from the subject. As the technology improves, it is quite likely that iris acquisition may take place from even greater distances and without any user involvement whatsoever.

From a privacy perspective these situations can conflict with the collection limitation, openness and purpose specification principles.

*DNA profiling*

Perhaps one of the greatest risks of DNA-based identification is the concern that "function creep" may allow DNA (deoxyribonucleic acid) identity information to be used for non-identity purposes. In conjunction with research on the humane genome, DNA profiling allows some health-related conclusions to be drawn, based on an individual's DNA composition. If a large-scale DNA-based identity system is constructed, there will likely be considerable pressure from prospective users of this information (insurance companies, financial institutions, researchers) to gain access to the DNA profile for risk analysis and research purposes.

***Biometric security issues***

In the security realm, we refer to three forms of verification: "something we know" (such as a password or personal identification number [PIN]); "something we have" (such as a smartcard or token); and "something we are" (such as a biometric).

While passwords and tokens may be improperly shared with others, your biometric attributes are difficult to transfer to another person (without surgical intervention). Used properly and responsibly, biometrics can add a high degree of assurance to a given system, especially when layered with one or both of the other forms of verification. These "multi-modal" forms of authentication (passwords together with tokens, tokens together with biometrics and even passwords together with tokens together with biometrics) allow the potential for a great deal of security and privacy enhancement.

Biometrics however, introduces a number of security risks that must be addressed in the implementation of any biometric system. Biometric systems have been shown to be susceptible to various types of attacks.

Some attacks require physical and logical access to the biometric system and scanner[6] (Soutar, n.d.). Another type of attack utilises a high definition print-out of an iris picture (Thalheim, Krissler and Ziegler, 2002), and yet another utilises nothing more than a "gummy bear" candy to facilitate the impersonation of another individual (Matsumoto *et al.*, 2002). Specific protections need to be architected into biometric systems to protect against these methods of security bypass. Liveness checking (commonly referred to as "anti-spoof measures"), when employed in the biometric scanner and the associated system can provide a significant degree of security enhancement.

Because of their static nature, biometrics are also susceptible to what is known as a "replay" attack. The response to a challenge such as, "what is your right index finger?" or "what does your face look like?" is always the same. Because of this, biometric system designers or implementers should ensure that biometric extraction and template generation processes are always seeded a random number that in effect turns the extraction into a unique secure event. A biometric sample or template generated at an earlier time could not be surreptitiously reintroduced into a biometric system using such protection.

It is important to remember that biometric-based technologies are only one component of an overall security system or identification system. We must always create appropriate backup and exception processing systems that utilise complementary and supplementary technologies so that our reliance on biometrics is appropriately measured against an overall system threat profile and respects the performance limitations of the technology. It is important to ensure that the security consequences of being improperly rejected by a system for accidental reasons (voice problem, scar on a finger, bandage, etc.) or just simply because of system error are appropriately considered. It could be said that overusing biometrics for inappropriately low value or low-risk transactions should be subject to cautious design.

There may be an expectation and temptation that the implementation of biometric systems may permit a reduction of manual and fallback processing and procedures. This is not the case; fallback and backup processing are ***even more important*** in the context of a biometric system and should be specifically accounted for in the system design.

Even with protections architected into biometric systems, some biometric-based technologies will likely require live human or video supervision of the biometric sample process to protect against certain security attacks on the biometric system (for example, using a different finger or an artificial mould (made of plaster or jelly) of a finger on a finger scanner, presenting a digital picture of a face or iris, etc.) or attempts by users to destroy or tamper with the biometric scanner.

It is also important to ensure that data cannot be "stolen" or "leak" from a biometric system either at the sensor or system database level. Biometric samples (images) and templates or feature datasets could be used for identity theft and impersonation attacks.

Multi-mode biometrics (two or more different biometrics used together in a biometric system, for instance – finger scanning together with iris scanning or face recognition together with hand geometry) can be used to increase both the security and accuracy of a biometric system. These systems can default to using only one biometric (for example, facial recognition) for everyday transactions and two biometrics (maybe facial recognition plus iris scanning) for higher value or special transactions when greater accuracy is required. By reducing the number of biometric interactions we can reduce the chance that data will be "stolen" or "leaked" from a system and still retain improved flexibility and accuracy.

### *Biometric inventory*

#### *Introduction*

The following section discusses the general functionality of a biometric system. A listing of major biometric technologies is included together with examples of system usage and research activities. Discussions regarding accuracy and performance of biometric technologies have been extracted from the biometric product testing performed by the Communications Electronics Security Group (CESG) in the United Kingdom (Mansfield *et al.*, 2001), from the Face Recognition Vendor Test,[7] the Fingerprint Verification Competition 2002,[8] and from vendor-supplied materials. Observations regarding ease of use and user acceptance are developed by the author, based on previous biometric implementation experience,

discussions with others in the industry and from the Sandia National Laboratories 1991 Biometrics Performance Evaluation (Holmes, Wright and Maxwell, 1991).

### Disclaimer

It should be noted that the above sources were selected due to their general availability and not because the author considers them especially accurate, applicable or relevant to a particular application or implementation. The testing protocol employed by the above sources may not be applicable to any or all applications.

### Accuracy

As noted above, observations regarding accuracy have been synthesised from the above noted publicly available biometric performance reports. The author has attempted to crudely approximate a single metric of "accuracy" based on measured false match rate, false non-match rate, equal error rate and other errors (failure to enrol, failure to acquire).

### Ease of use

"Ease of use" represents the ease with which an individual being identified or authenticated may interact with a biometric system. This measurement is largely objective and is dependant upon the type of device used to capture the biometric (camera, scanner, etc.). In real life applications, there may be somewhat of a trade-off between "ease of use" and "accuracy". Ease of use has been approximated based on the author's personal experiences with the technology, discussion with industry colleagues and review of background documentation (sources noted above; ICAO, 2003b).

### User acceptance

"User acceptance" describes the degree to which individuals tend to have concerns and objections to the use of a specific biometric. In some countries facial recognition is poorly accepted as women's faces are generally covered; in others finger scanning has connotations of criminality. This measurement is largely subjective and will vary from person to person and from country to country depending on the data protection regime in pace, the cultural context and the expectation of the individual. User acceptance has been approximated based on the author's personal experiences with the technology, discussion with industry colleagues and review of background documentation noted above. This measurement is time dependant and may change in the future. Given the context specific and subjective nature of user acceptance, this characteristic may complicate social and political factors for biometric implementations. This may, in fact, be a strong motivator for regulatory work in this area.

### Stability

"Stability" represents the degree to which a biometric trait remains constant through the normal development and aging process of an individual. The less "stability" a trait has, the more likely that updating or re-enrolment of the individual will be required.

Transparency

"Transparency" is the degree to which the knowledge of the data subject is required for the biometric collection to take place. Some biometric-based technologies (facial recognition, some forms of iris scanning, gait recognition, etc.) allow collection without the knowledge or consent of the individual. Transparency provides an indication of the covert potential of a given biometric technology. Some projects, such as the Defense Advanced Research Projects Agency (DARPA) "Human ID at a Distance" project, specifically focus on biometric-based technologies that may be operated in a covert manner.[9]

*Biometric system operation*

The information flow of a biometric system may be summarised as follows:

- Biometric sample collection.
- Biometric feature extraction.
- Biometric template or feature dataset creation.
- Biometric template or feature dataset matching.

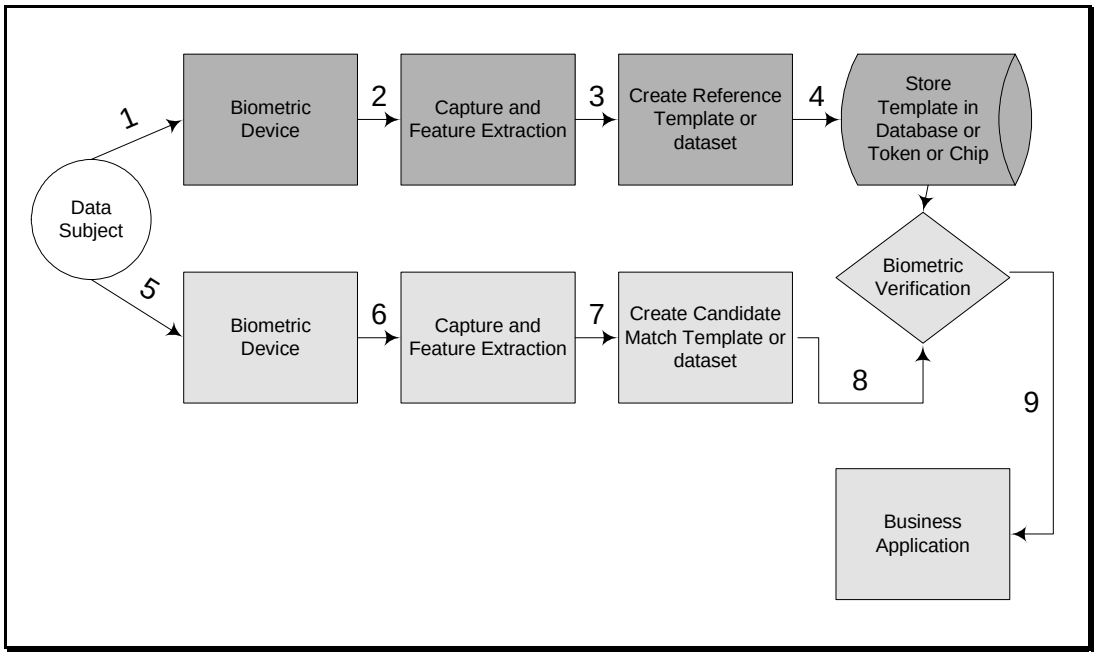
The process of feature extraction and template or feature dataset creation is an irreversible process. It is not possible to recreate a raw biometric sample (such as an image of a face, iris, retina or finger) from a biometric template or feature dataset. As of today, most biometric systems are only able to interoperate using the raw biometric sample. Where the biometric sample is destroyed after collection (perhaps to enhance the privacy protectiveness of a given system) this will limit interoperability. In the future, the standardisation and the normalisation of biometric templates could enable the interoperability of systems using these templates just as in the case of raw biometric samples. While standardisation should always be encouraged, one should be aware that unless interoperability and privacy protection are ***both*** achieved, there is a direct trade-off between interoperability and the privacy protection *de facto* afforded by the non-interoperability (this trade-off will apply equally to both the case of retention of raw biometric samples and biometric templates). *(Note: this may, in fact, be the intention of the system designer working to follow the "finality principle" in preventing interfaces to other systems.)*

The two matching modes of a biometric system are:

- One to many (1:N, also known as biometric search or biometric identification or recognition): One to many searches are designed to determine identity based solely on biometric information. One to many matching answers the question, "Who am I?" In systems supporting one to many searches a central database must be built containing all biometric templates enroled in the system. This database is used to perform the one to many search.
- One to one (1:1, also known as biometric verification, matching or authentication): The process of establishing the validity of a claimed identity by comparing a verification template to an enrolment template. Verification requires that an identity be claimed. One to one matching answers the question, "Am I whom I claim to be?" One to one matching does not ***require*** a central database to be built, if the comparison is made against a template stored in a personal device retained by the individual whose identity is to be verified.

Figure 1 describes the common components of a biometric system.

Figure 1. **Biometric system design**




*Note*: The biometric enrolment process is shown in dark grey, the biometric verification or search process is shown in light grey.

Enrolment process

During enrolment, the subject uses *(1)* a biometric device (*e.g.* such as a finger scanner) to provide a biometric sample. *(2)* The biometric system will extract feature information from the biometric sample. After this point, the original biometric sample (*e.g.* image of finger) may be discarded in a privacy protective manner. (As noted above, this will limit the interoperability of the biometric system.) The biometric feature information is then formatted *(3)* into a template or feature dataset. This template or feature dataset is then stored *(4)* in a centralised biometric database, or in a distributed system on a token (smart-card or magnetic stripe card) in the user's possession.

Verification or search process

During search or verification, the subject uses *(5)* a biometric device to provide a biometric sample *(6)*. The biometric system will extract feature information from the biometric sample. After this point, the original biometric sample may again be discarded in a privacy protective manner. The biometric feature information is then formatted *(7)* into a template or feature dataset to be used to perform a search or verification. This template or feature dataset is now submitted *(8)* to the biometric verification engine. In the case of a search, the search candidate is compared to all biometric samples stored in the system, generating zero to many possible matches; for a verification a one to one comparison is made against the suspected identity and generates a pass/fail output. Usually, some form of interconnection *(9)* to a business application is utilised to process the output of the biometric system.

*Scientific method / biometric testing*

> "The real purpose of the scientific method is to make sure Nature hasn't misled you into thinking you know something you don't actually know."
>
> - Robert M. Pirsig, *Zen and the Art of Motorcycle Maintenance.*

It is especially important when we consider new technologies, to make sure that the science behind each technology stands up to scrutiny ***and*** that it supports what we think it supports. There is general misapprehension among governments and the general public about the abilities and accuracy of biometric technologies (McMilan, 2002).

A recent presentation by Jim Wayman, Director of the Biometric Test Center at the San Jose State University concluded that, "the hype is factually correct, but leaves an impression that may not be accurate" (Wayman, 2002). Reinforcing the appearance that the public is yearning for a magic-bullet biometric solution, in the aftermath of the attack on the World Trade Center, the stock value of some biometric vendors increased substantially (Visionic's stock price, for example, has tripled since the event [*Business Week*, 2002]). Riding this wave of public interest, some vendors even began offering their respective products as a solution for crime and terrorism only a day after the horrific events of September 11th, 2001 (AcSys Biometrics, Corp. and Nexus Group International Inc., 2001).

In a paper on facial recognition, Roger Clarke of the Australian Privacy Foundation noted, "the technology, and products using it, have been subjected to insufficient testing by independent laboratories. The performance of actual installations has not been subjected to critical evaluation by uninterested analysts, and results even of the limited tests performed have generally been hidden from view" (Clarke, 2003). Dr. Clarke admonishes us that, "such limited information as is available suggests that the technologies have performed atrociously badly" (Clarke, 2003).

There are a great many performance metrics for biometrics. Some are measured directly from operation of the biometric system and others are derived from these measurements. Unfortunately there is no single metric that indicates how well a system will perform in all circumstances and environments. Analysis of multiple metrics is necessary to determine the strengths and weaknesses of each technology and vendor under consideration for a given application. The selection and interpretation of specific metrics is a non-trivial exercise and requires considerable expertise.

It should also be noted that the specifics unique to each implementation (for instance, the population size, the biometric selected, the environment, the manner of identification and authentication) will have a great effect on performance metrics. Testing which generates system performance metrics is most valuable when it emulates real-world application environments.

*Biometric performance measurements*

Every biometric technique has a different method of assigning a "score" to the biometric correlation (the degree to which the candidate biometric sample matches a previously enrolled biometric sample); a "threshold value" is defined which determines when a match is declared. Scores above the threshold value are designated as a "match" and scores below the threshold are designated as "non match". As previously noted, this correlation is a statistical function based on the biometric type, the hardware and software, the algorithm and the operational settings of the system. A given correlation may or may not be "accurate" depending upon the circumstances.

"False reject rate"

The "false reject rate" measures the extent to which a given biometric system will fail to match a correct input (a legitimate user is rejected).

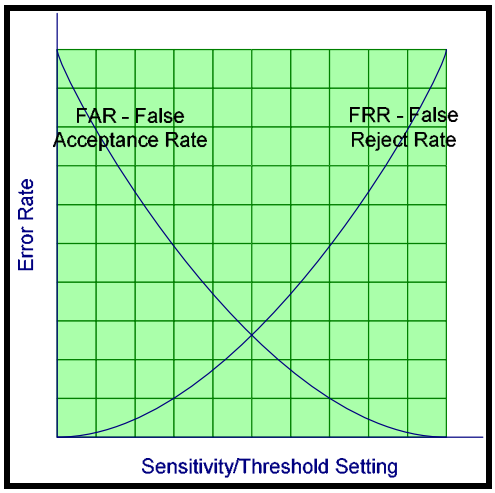
"False acceptance rate"

The "false acceptance rate" measures the extent to which a given biometric system will match on an incorrect input (an impostor will be accepted as a valid match).

"Equal error rate"

The "equal error rate" or crossover accuracy rate measures the point of intersection of the false acceptance and false rejection error curves. In general, as the value of the crossover accuracy increases (lower error rate at crossover) the inherent accuracy of the biometric increases. Figure 2 contains an example of an error crossover curve.

Figure 2. **Biometric system error trade-off curve**

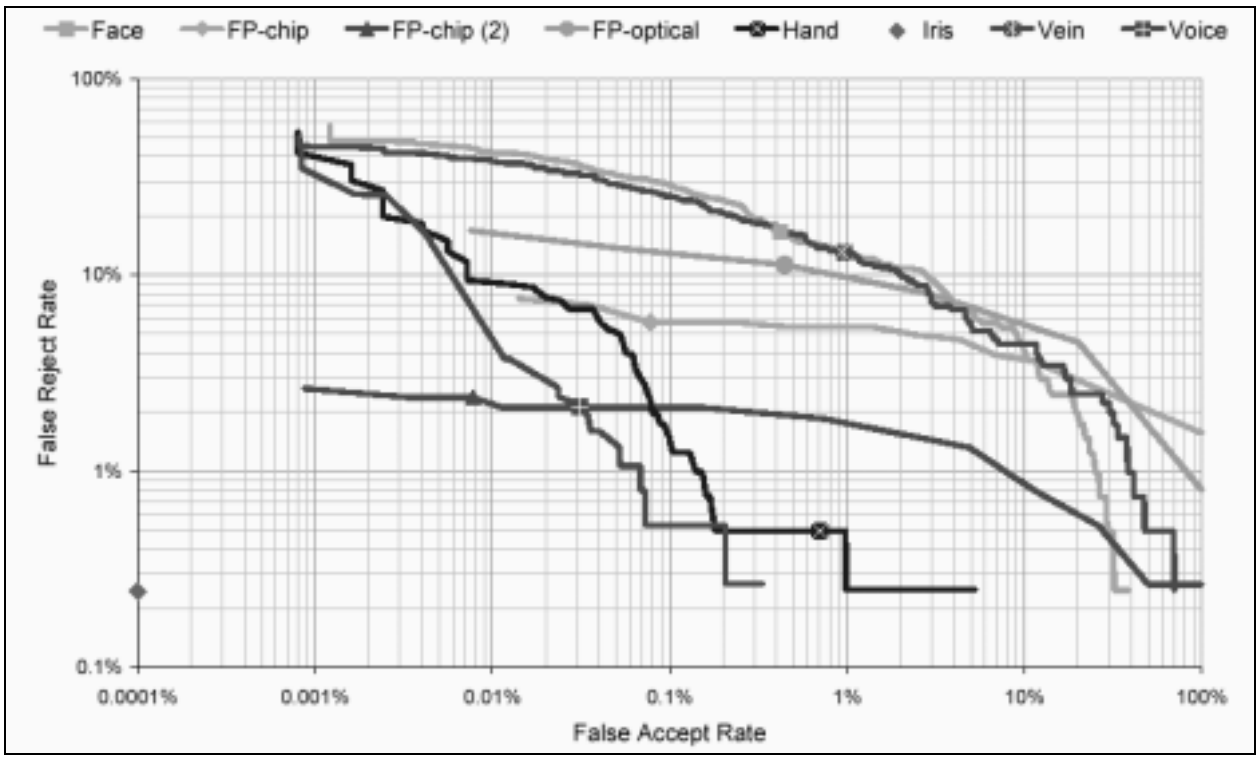



*Source*: Mansfield, T. *et al.* (2001), "Biometric Product Testing Final Report", CESG report, 19 March, www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf, accessed 20 April 2004.

Biometric system error trade-off

As we can see from Figure 3 below, for all biometric technologies (with the exception of iris scanning which has preset error and accuracy values) the performance characteristics may be adjusted over a wide range of error values. Decisions may be made by the system designer and operator to adjust accuracy based on the nature of the system (if the system is designed to control access or prevent duplicate enrolment) and the degree to which exception processing can be tolerated (the handling of false matches and failures of legitimate users).

Figure 3. **Example biometric system error trade-off curve**




*Note :* This figure is taken from the CESG evaluation made in 2000 with a limited number of participants: this figure is for illustration purposes only; actual performance of individual biometrics will vary depending upon context.

*Source*: Mansfield, T. *et al.* (2001), "Biometric Product Testing Final Report", CESG report, 19 March, www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf, accessed 20 April 2004.

*Other performance measures*

"Failure to acquire"

The "failure to acquire" rate measures the proportion of attempts for which a biometric system is unable to capture or locate an image of sufficient quality. For example, if a system is unable to capture the image of a face against a given background, or if a user has injured their finger and a scar or bandage is obscuring features on the finger.

"Failure to enrol"

The "failure to enrol" rate measures the proportion of individuals for whom the system is unable to extract sufficient features and generate repeatable templates. This includes those unable to present the required biometric feature (for example a finger scan from a user who has no fingers), those unable to produce an image of sufficient quality at enrolment, as well as those unable to reproduce their biometric features consistently. Some individuals through genetic anomaly lack sufficient detail and features on their fingers to allow a biometric template to be constructed. Often older users will be prone to "failure to enrol" errors as the elasticity and thickness of the skin changes with age.

Throughput

"Throughput" measurement is the rate at which biometric identification and authentication may be performed. This metric is comprised of two components, the acquisition and extraction time, and the search and match time. In very large biometric systems with very large enrolment populations, throughput times may become critical to the successful operation of the system.

System cost

The cost of a system includes not only the cost of hardware and software, but also the ongoing operational costs and any costs associated with performance errors. If a 1:N identification system is tuned to minimise false rejections, it will likely generate a greater number of false acceptances (the system will think you might be someone else), which will require manual follow-up. Similarly, if a 1:1 verification system is tuned to minimise false acceptance (someone else claiming to be you), it will likely generate a greater number of false rejects (rejecting legitimate users) and requiring a manual override or exception process. There will always be a cost impact from the system-tuning decision.

*Physiological biometrics*

Physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body.

As noted above, the degree to which a biometric may be collected in a covert or overt manner may limit or enhance the opportunity for the user to clearly express their consent (for instance with finger-scanning, the user may express their consent clearly by placing a finger on a scanner, with retinal-scanning the user may express their consent by looking into a retinal scanner, etc.).

As we review the inventory of physiological biometrics, it is important to remember that, to the extent possible, our preference is always to incorporate a clear expression of user consent in the biometric collection process.

**FINGER-SCANNING**

Functionality

It has long been known that the skin ridge patterns on fingers (and elsewhere) can be used to uniquely identify people. A classification scheme to aid in matching people against stored records was developed in the 1890s. Although much research has taken place, the science of forensic fingerprint identification traces its roots back over 100 years.

This scheme is based on the recognition of certain types of "features". The major features are the arch, loop and whorl. Each finger has at least one major feature. The smaller or minor features (or minutiae) consist of the position of ridge ends and ridge bifurcations. There are between 50 and 200 such minor features on every finger. This provides a great deal of information for feature extraction and produces a minutiae which is usually 250-700 bytes (see Figure 4).

Figure 4. **Fingerprint features**

Most biometric vendors utilise minutiae in some fashion. Those who do not utilise minutiae use pattern matching, which extrapolates data from a particular series of ridges. This series of ridges used in enrolment is the basis of comparison, and verification requires that a segment of the same area be found and compared. The use of multiple ridges reduces dependence on minutiae points, which tend to be affected by wear and tear. The templates created in pattern matching are generally, but not always, two to three times larger than in minutiae - usually 900-1 200 bytes.

Accuracy

Accuracy is high and has the potential to be very high if desired, by using additional fingers in the enrolment and matching process. Flexible performance tuning and configuration can accommodate a wide range of applications. Depending upon the application, systems are usually tuned to tolerate a higher false positive error rate at the expense of false negative error rate. Vendors claim low error rates, but super large size populations may require binning techniques or will multiple finger scans to maintain even acceptable performance.

Ease of use

When prompted, the user will place his or her finger on a small optical or capacitive scanning surface. This surface is built into a peripheral device, mouse, keyboard or special purpose PCMCIA (Personal Computer Memory Card International Association) card. The user generally must hold the finger in place for one to two seconds, during which the biometric capture and feature extraction will take place. Finger scanning is rated with a “High” ease of use.

User acceptance

Although common and accepted in some parts of the world, finger-scanning maintains an element of negativity due to its association with fingerprinting and the criminal justice system. User acceptance is rated “Medium Low”.

Stability

The ridges and features of our fingerprints are stable over time. They may, however, be damaged due to heavy use or injury and sometimes the elderly may suffer from a lack of differentiation on their fingers (difficulty in feature extraction due to thin skin). Notwithstanding these problems, stability is rated “High”.

Examples of existing applications

*Government/immigration*

- The European Union (EU) recently brought the Eurodac system on line, the large-scale centralised fingerprint database will allow any member country to check the fingerprints of asylum seekers against the records of other EU countries. If an asylum seeker has already claimed asylum in another EU country, they will be returned to have their claim dealt with there (EC, 2003).[10]
- Many states perform finger-scanning on new applicants for social services benefits or other human service programmes. This protects against a type of fraud known as "double dipping", the practice of enrolling for a benefit under multiple names. New York State has over 900 000 people enrolled in such a system.

*Education*

- In Pennsylvania, finger-scanning is being used in a school lunch programme (*eSchool News*, 2001).
- In Minnesota, finger-scanning is also being used in a school library (*eSchool News*, 2000).

*Online/network authentication*

- Finger-scanning is starting to be incorporated into personal computing devices to provide user authentication. Hewlett-Packard recently introduced a personal digital assistant (PDA) which incorporates a biometric sensor for finger-scanning and can restrict access to authorised users only (Hamilton, 2003).
- Other manufacturers, such as Asian computer giant Acer Inc. and International Business Machines Corp. (IBM) have built finger-scanning devices into their notebook computers.
- Targus Inc., the leader in computer accessories, currently sells a PC card fingerprint reader — the "DEFCON Authenticator" — for use with laptops and a reader "pod" that can connect to any computer through a USB connection.

**HAND GEOMETRY**

Functionality

Hand geometry is currently among the most widely used biometric technologies, most suitable for access control and time and attendance applications. As opposed to more exotic biometric technologies, whose implementations may be quite few and far between, hand scanning is used reliably at thousands of places of employment, universities, apartment buildings, and airports – any place requiring reasonably accurate, non-intrusive authentication. The nature of hand geometry technology is such that most projects are fairly small scale and involve only a handful of readers, but there are some projects which incorporate dozens of readers.

This technique uses a three-dimensional image of the hand and measures the shape, width and length of fingers and knuckles. A user places a designated hand on a reader, aligning fingers with specific positioned guides. A camera is used to capture both a top view, which gives length and width information, and a side view, which gives a thickness profile (see Figure 5). The template that is generated is an economical 10 bytes or less.

Figure 5. **Hand geometry scanner**

*Source*: Wilson, Bill (1992). "Hand Geometry Boasts Simplicity, Convenience", *Access Control*, March, reprint, p. 1.

Accuracy

Accuracy can be high if desired, and flexible performance tuning and configuration can accommodate a wide range of applications. Hand geometry is better suited to one-to-one verification applications.

Ease of use

The user places his/her hand, palm-down, onto a metal scanner (shown above) with five finger guidance pegs. The pegs ensure that fingers are placed properly ensuring correct hand positioning. Hand geometry is rated as "High" ease of use.

User acceptance

User acceptance of hand geometry is rated "Medium-High".

Stability

Hand geometry is rated as "Medium-High" stability. The shape and features of one's hand will change slowly over the lifetime.

Examples of existing applications

*Government/immigration*

- Perhaps the best-known government application is the US Immigration and Naturalization Service's Passenger Accelerated Service System (INSPASS). Until its recent suspension,[11] INSPASS allowed frequent travellers to circumvent long immigration lines at international airports in Los Angeles, Miami, Newark, New York, Washington DC, San Francisco, Toronto and Vancouver. Qualified passengers, after enrolling in the service, received a mag-stripe card encoded with their hand scan information. Instead of being processed by passport control personnel, INSPASS travellers would swipe their card, place their hand, and proceed directly to the customs gate. INSPASS enrolment exceeded 60 000 persons.

- The Mexican government utilises hand geometry to administer an attendance control system in the Land Reform Ministry. This system functions across six separate facilities and interfaces with the payroll registry system.

*Education*

- The University of Georgia uses the technology to control access to its student cafeteria. When students visit a cafeteria, they swipe their identity cards through a reader and have their hands verified before being able to enter the food service area (Zunkel, 1994).
- An American elementary school uses the technique to identify individuals picking up children. Anyone authorised by the parents can enrol in the system. To be able to pick up a child from the school, a person first must be verified by a hand geometry reader (IR Recognition Systems, 1998).
- In Toronto, Canada, hand geometry is used by a racquet and fitness club[12] to verify the identity of 12 000 club members and staff.

*Private sector*

- In Ontario, Canada, hand geometry is used at nuclear power generating stations (Milroy, 1998).
- In the United States, hand geometry scanners verify identity at the front entrances of over half of the nuclear power plants (findBIOMETRICS.com, n.d.).

*Other*

- The 1996 Summer Olympic Games in Atlanta used hand geometry to identify and secure approximately 150 000 athletes, staff, and other participants (Tomko, 1996). This biometric system was integrated with the Olympic Village security system to process millions of transactions, with minimum delay (findBIOMETRICS.com, n.d.).
- The US Federal Bureau of Prisons uses hand geometry to track movements of its prisoners, staff and visitors within prisons. Once a person enters the system, they must have their hand scanned. The information is put in a database and the person is issued a magnetic swipe card that they carry at all times. Prisoners are enrolled for access control to places such as the cafeteria, hospital and recreational lounges (Chua, 2001).

### FACIAL RECOGNITION

Functionality

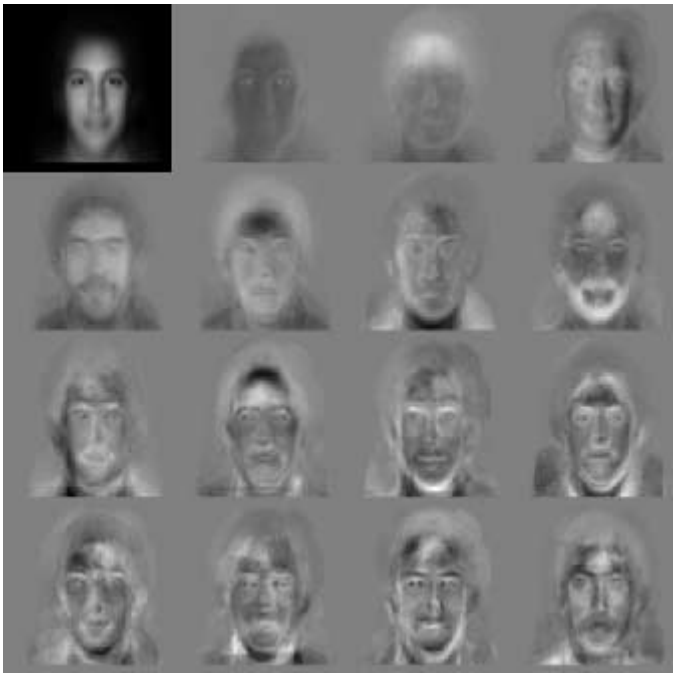
Enrolment generally consists of a 20-30 second enrolment process whereby several pictures are taken of one's face. Ideally, the series of pictures will incorporate slightly different angles and facial expressions, to allow for more accurate matching. After enrolment, distinctive features are extracted (or global reference images are generated), resulting in the creation of a template. The template is much smaller than the image from which it is derived: facial images can require 20-40 kb, templates range from 100 bytes to 3 500 bytes. The smaller templates are normally used for 1:N (one to many) matching.

Depending upon the vendor, one of four primary methods is employed to identify and verify subjects. These are, eigenfaces, feature analysis, neural network, and automatic face processing.

*Eigenface* – roughly translated as "one's own face" – is a technology patented at the Massachusetts Institute of Technology (MIT) (MIT, 2002) which utilises two dimensional, global greyscale images

representing distinctive characteristics of a facial image. Variations of eigenface are frequently used as the basis of other face recognition methods (see Figure 6).

Figure 6. **Standard eigenfaces**



*Source*: MIT (2002), "Photobook/Eigenfaces Demo", http://vismod.media.mit.edu/vismod/demos/facerec/basic.html, accessed 20 April 2004.

*Feature analysis* is perhaps the most widely utilised implementation of facial recognition technology. This technology is related to eigenface, but is more capable of accommodating changes in appearance or facial aspect (smiling vs. frowning, for example). Identix, a prominent facial recognition company, uses local feature analysis (LFA).[13] LFA is a mathematical technique developed by co-founders of Visionics Corporation, and is based on the realisation that all facial images (for that matter all complex patterns) can be synthesised from an "irreducible set of building elements", a sort of atomic facial building blocks. LFA utilises dozens of features from different regions of the face, and also incorporates the relative location of these features. The extracted features are building blocks, and both the type of blocks and their arrangement are used to identify/verify.

LFA is resistant to changes in lighting, skin tone, eyeglasses, facial expression and hair and is robust with respect to pose variations, up to 35 degrees in all directions.[14]

*Neural network:* Using this technology, features from both faces – the enrolment and verification face – vote on whether there is a match. Neural networks employ an algorithm to determine the similarity of the unique global features of verification face versus enrolment faces, using as much of the facial image as possible. An incorrect vote, *i.e.* a false match, prompts the matching algorithm to modify the weight it gives to certain facial features. This method, theoretically, leads to an increased ability to identify faces in difficult conditions.

*Automatic face processing:* (AFP) is a more rudimentary technology, using distances and distance ratios between easily acquired features such as eyes, end of nose, and corners of mouth. Though overall not

as robust as eigenface, feature analysis, or neural network, AFP may be more effective in dimly lit, frontal image capture situations.

Accuracy

Although accuracy can be high if desired, actual system performance is more likely determined by the number of false positives or duplicate matches a given application can tolerate. Actual trials with facial recognition systems indicate difficulty in maintaining good performance with acceptable error rates.

Ease of use

The user will face the camera, preferably positioned close to the face. In some situations, the user may need to alter his facial aspect slightly to ensure correct biometric acquisition. Facial recognition is rated as "Medium-High" ease of use.

User acceptance

User acceptance of facial recognition is rated "High" given the non-invasive nature of the biometric capture.

Stability

Facial recognition is rated as "Medium-Low" stability. Depending upon the type of facial recognition employed, a system may be better able to cope with the ongoing facial changes we experience over a lifetime.

Examples of existing applications

*Government/immigration*

- Recent press coverage in the United Kingdom, reports that "Security cameras will be able to zoom in on the faces of drivers entering London's congestion charge zone as part of a sophisticated 'ring of steel' around the capital." The article indicates that the new facial recognition system is designed to protect the city from a terrorist attack and allows hundreds of cameras to register individual faces while the images are being cross-referenced to intelligence and police databases of various suspects. UK defence experts indicate that the new system "could thwart a truck or car bomb, believed to be at the top of al-Qaeda plans in Britain" (Townsend and Harris, 2003).
- Japan's Ministry of Land, Infrastructure and Transport is conducting a trial using contact-less integrated circuit (IC) chips in conjunction with facial recognition *and* iris recognition to help accelerate the time it takes to check in at Japanese airports (Miyake, 2002).
- The Australian Customs Service started a trial in the summer of 2002 of SmartGate, a facial recognition system which matches against passport photographs (Australian Justice and Customs, 2002).
- Since the events of September 11th, considerable interest has been expressed in utilising facial recognition to aid in the recognition of terrorists and other criminals.[15]

*Banking*

- Some American banks, gas stations and convenience stores are using this technology to identify and record cheque-cashing transactions (*Biometric Technology Today*, 1998). One American automatic teller machine (ATM) system automatically takes a "biometric" picture every time a customer cashes a cheque. The customer first has to enrol in the system, but no bank account or driver's license is needed. In order to cash a cheque, customers key in their social security numbers. This information, combined with the biometric, creates a real-time, permanent record of the transaction (*Biometric Digest*, 1998).
- German banks have been using face recognition technology to give customers unattended, 24-hour access to their safety deposit boxes. Customers request their boxes at a self-service computer terminal, which includes a video camera. The camera captures and processes the customer's facial image. System software verifies the person's identity and authority to receive the requested safety deposit box. If the person is authorised, the box is retrieved by robots and delivered to the owner by an automated handling system (Burnell, 1997).

*Travel*

- A Malaysian company is using this technology to create an airport security system that tracks passengers' baggage with an image of their face. Only when passengers actually enter the plane will the system allow their baggage to be loaded (Belsize, 1997).
- Some casinos are using face recognition as a way of identifying suspicious players. A surveillance camera captures an image of the individual's face and then compares it to a digitised photo database of "known cheaters".

*Online/network authentication*

- There also are applications that replace passwords for computer log-in. The primary advantage is that face recognition is able to operate "hands-free." With a camera positioned on a computer monitor the user's identity is verified simply by staring at the screen. Access to sensitive information can be disabled when the user moves out of the camera's field of vision.

*Other*

- In January 2000, the Tampa Police Department conducted one of the largest facial recognition test at Super Bowl XXXV in Tampa Bay, Florida (Bonsor, n.d.).

### IRIS SCANNING

Functionality

Iris scanning employs the unique characteristics and features of the human iris in order to verify the identity of an individual. The iris is the area of the eye with a pigmented or coloured circle, usually brown or blue, which rings the pupil of the eye.

Each iris has a unique and complex pattern such that even a person's right and left iris patterns are completely different. It has been claimed that the system is "foolproof" (Golgotha, 1999) because artificial duplication of the iris is virtually impossible due to its properties and the number of measurable characteristics. The iris is stable throughout one's life and is usually not susceptible to wear and injury (given that the user has a vested interest to protect it). Ordinary contact lenses do not interfere with the use of this biometric identifier and vendors claim (RYCOM Inc., n.d.) that coloured contact lenses do not interfere as well, even though there is little independent research on the issue. Iris recognition technology involves the use of a high resolution camera and a light source to capture a digital image of the iris. Since

about 85% of the iris is normally visible (with the remainder being covered by the eyelids), no invasive measures are needed to acquire an image of the iris. This type of biometric technology can be used for one-to-one verification or one- to-many recognition (Roethenbaugh, 1998b).

The template size for iris scanning is approximately 500 bytes.

Accuracy

Unlike other biometrics, iris scanning maintains an extremely low error rate across the spectrum of system configuration. It is rated "Very High" for accuracy.

Ease of use

The user positions him or herself near the acquisition device (peripheral or wall mounted camera). The user will centre the eye on the device so that the reflection of the eye is visible. Depending on the device, the user is between 4-24 inches away. Capture and feature extraction are nearly immediate. Iris scanning will eventually become very easy to use, but as of today, it is still one of the more complex biometrics. Rated as "Medium-Low" for ease of use.

User acceptance

User acceptance of iris scanning is rated "Medium-High" given the non-invasive nature of the biometric capture. As the technology improves, greater capture distances are possible, this is likely to increase.

Stability

Our irises are extremely stable over the course of our lifetime. This biometric is rated at "High" stability.

Examples of existing applications

*Government*

- CANPASS – Air: A joint initiative of the Canada Customs and Revenue Agency (CCRA) and Citizenship and Immigration Canada that will facilitate efficient and secure entry into Canada for pre-approved, low-risk air travellers. This voluntary registration programme utilises iris scanning to confirm passenger identity.[16]

*Banking*

- Some ATM manufacturers include iris scans as an alternative to passwords or PINs. In May 1999, Bank United of Texas became the first bank in the United States to offer iris recognition at ATMs.
- Iris scanning technology is already utilised by over a dozen different banks outside of the United States (*Mercury News*, 1999).
- The Royal Bank of Canada and the Canadian Imperial Bank of Commerce tested an ATM with iris scanning capabilities in Toronto (Bonier, n.d.).

*Education*

- A Tae Kwon Do chain in the United States uses iris recognition to speed up its daily sign-in and information-processing procedures. A one-second glance into a camera for verification of identity is necessary each time a student enters a class (Iridian Technologies, Inc. n.d.).

*Travel*

- Amsterdam's Schiphol airport is claiming success with a biometric security system that uses iris scanning in conjunction with a special card to allow passengers to bypass traditional passport control (CNN, 2000). Frequent flyers can sign up for the "Privium Club" which uses software and hardware developed by Schiphol, the airport police and the immigration service (Chua, 2001). Members have their iris data entered on a chip of an identification card. The passenger can zip through passport control and check-in by looking into a scanner. The scan is also used for airport personnel in secure areas.
- An iris scanning biometric system designed by EDS is under trial at Israel's Ben Gurion Airport (Delaney and Prada, 2002).
- Japan's Ministry of Land, Infrastructure and Transport is conducting a trial using contact-less IC chips in conjunction with facial recognition *and* iris recognition to help accelerate the time it takes to check in at Japanese airports (Miyake, 2002).

## RETINAL SCANNING

Functionality

Retinal scanning looks at the vascular patterns found on the fundus or the inside rear surface of the eye. Since no two retinas are the same – even in identical twins – an individual can be distinguished from others based on the vascular pattern observed.

Retinal scanners direct a beam of light into the eyeball and record the pattern of veins in the eye. Given the invasive nature of biometric sample acquisition, and the need for active user participation and consent, some regard retinal scanning as more privacy protective than iris scanning (Pigg, 2002).

Template size for retinal scanning is approximately 100 bytes.

Accuracy

Accuracy is rated as "Very High".

Ease of use

The user will look into a small opening on a desktop or wall mounted device. The user will hold their head very still, while looking at a green light located within the device. Typical capture and extraction time is 6-10 seconds. Retinal Scanning is also one of the more complex biometrics. It is rated as "Low" for ease of use.

User acceptance

User acceptance of retinal scanning is "Low". There is some user concern about the health effects of introducing light into the eye for scanning purposes. According to the Sandia Report, retinal scanning had the most negative reaction compared to all other biometric techniques. The "users have... concerns about

retina identification, which involves shining an infrared beam through the pupil of the eye" (Holmes, Wright and Maxwell, 1991).

Stability

The retina is extremely stable over the course of our lifetime. This biometric is rated at "High" stability.

Examples of existing applications

*Other*

- Due to the perceived invasiveness and high cost, retinal scanning is not widely utilised outside of specialised high-security and national security applications.

**FINGER GEOMETRY**

Functionality

This technology operates on similar principles as hand geometry, but utilises only one or two fingers. Measurements of unique finger characteristics, such as width, length, thickness and knuckle size are taken.

Finger geometry systems can perform one-to-one verification or one-to-many identification. The main advantage is that these systems are fast and designed to accommodate "a high throughput of users" (Roethenbaugh, 1998b). According to one company, its system confirms identity within one second (Biome Partners, Inc., 1999). Finger geometry systems are considered very durable and able to cope well with external conditions (Roethenbaugh, 1999). As an example, Disney World uses three-dimensional two-finger geometry to verify the identity of season ticket holders in the United States (James, 1997).

Accuracy

Accuracy is rated as "Medium". Not suitable for one-to-many applications.

Ease of use

Like hand geometry, this biometric uses a special hand scanner upon which the user will lay the finger, or a hole into which the user will insert the finger. This biometric is rated with "High" ease of use.

User acceptance

User acceptance of finger scanning is rated "Medium-High" given the non-invasive nature of the biometric capture. Some systems, which require a user to insert their finger completely into a hole, can cause greater user resistance.

Stability

Finger geometry is rated as "Medium-High" stability. The shape and geometry of a finger may change slowly over the course of our life.

*Behavioural biometrics*

**VOICE RECOGNITION**

Functionality

Voice recognition technology utilises the distinctive aspects of the voice to verify the identity of individuals. Voice recognition can utilise any audio capture device, including wireless and wireline telephones and microphones. The performance of voice recognition systems can vary according to the quality of the audio signal as well as variation between enrolment and verification devices, so acquisition normally takes place on a device likely to be used for future verification.

During enrolment an individual is prompted to select a passphrase or to repeat a sequence of numbers. The passphrases selected should be approximately 1-3 seconds in length – very short passphrases lack enough identifying data, and long passwords have too much, both resulting in reduced accuracy. The individual is generally prompted to repeat the passphrase or number set a handful of times, making the enrolment process somewhat longer than most other biometrics. The common template size for voice recognition is 4 000-10 000 bytes.

Voice verification is technically considered a hybrid behavioural and physiological biometric because the voice pattern is determined, to a large degree, by the physical shape of the throat and larynx, although it can be altered by the speaker.

One-to-one verification is the preferred application. The technology is easy to use and does not require a great deal of user education. In 1997, when one Canadian bank undertook customer surveys on the acceptability of biometrics, the one technique that was not rejected was voice recognition (Baker, 1997).

Accuracy

Accuracy is rated as “Medium”. Not usually suitable for one-to-many applications. Changes in the human voice due to illness can sometimes present problems.

Ease of use

Using a telephone or microphone, the user will recite an enrolment or pass phrase when instructed. Voice recognition is rated as “High” ease of use.

User acceptance

Voice recognition acceptance is “High”.

Stability

Voice recognition is rated as “Medium-Low” stability given the tendency of our voice to change over time.

Examples of existing applications

*Government/immigration*

- Voice recognition has been implemented in physical access solutions for border crossing purposes (Jackson, 1997).

*Banking*

- Voice recognition also is being integrated into security systems for online banking and electronic commerce (PR Newswire, 1999a).

*Online/network authentication*

- In May 1999, it was announced that more than 5 000 personal computers with speaker verification systems had been sold on the Home Shopping Network since mid-April (PR Newswire, 1999b).

*Other*

- One European automobile manufacturer even investigated the possibility of incorporating speaker verification into its ignition systems (Cole, 1995).

**DYNAMIC SIGNATURE VERIFICATION**

Functionality

This behavioural biometric involves the analysis of the way in which a person signs his/her name. Signature biometrics are often referred to as dynamic signature verification (DSV). With this technique, the manner in which someone signs is as important as the static shape of their finished signature. For example, the angle at which the pen is held, the time taken to sign, the velocity and acceleration of the signature, the pressure exerted, and the number of times the pen is lifted from the paper, all can be measured and analysed as unique behavioural characteristics (Rosen, 1990). As DSV is not based on a static image, forgery is considered to be difficult.

Signature data can be captured via a special pen or tablet, or both. The pen-based method incorporates sensors inside the writing instrument, while the tablet method relies on sensors imbedded in a writing surface to detect the unique signature characteristics. Recently, another variation has been developed known as acoustic emission. This measures the sound that is generated as an individual writes their signature on a paper document (Association for Biometrics and International Computer Security Association, 1998). Template size for voice recognition is approximately 1 500 bytes.

Accuracy

Accuracy is rated as “Medium”. Not usually suitable for one-to-many applications. Dynamic signature verification has the same problem with match discrimination (*i.e.* finding a match in a large database) as does hand geometry.

Ease of use

When prompted, the user will sign their name on an electronic capture device. Dynamic signature verification is one of easiest biometrics to use; it is rated “High”.

User acceptance

Dynamic signature verification acceptance is “Medium-High”.

Stability

Dynamic signature verification is rated as “Medium-Low” stability given the tendency of our signature to change over time.

Examples of existing applications

*Banking*

- The Chase Manhattan Bank has tested DSV to identify corporate clients initiating transactions.

*Private sector*

- A number of American hospitals, pharmacies and insurance firms use this biometric technique to authenticate electronic documents.

*Other biometrics*

The following biometric technologies are, in the author’s opinion, too experimental or in need of future development to be considered ready for practical application today. They are included to give an appreciation of the research direction for future development.

**EAR GEOMETRY**

Functionality

A lesser-known physiological biometric is the shape of the outer ear, lobes, and bone structure (Association for Biometrics and International Computer Security Association, 1998). Apparently, police are able to capture earprints of criminals left when they listen at windows and doors. The technology has been used to obtain convictions in the Netherlands (*The Toronto Star*, 1995). One French company is working on the “octophone”, a telephone-like biometric device that captures images of the ear (McMurchie, 1999).

**BODY ODOUR MEASUREMENT**

Functionality

This biometric analyses human body smell; sensors are capable of capturing body odour from non-intrusive parts of the body such as the back of the hand, arm or neck. Each unique human smell is made up of chemicals which are extracted by the system and classified into a template (Roethenbaugh, 1998b). Reportedly, the University of Cambridge has developed an “electronic nose” that can identify people by their distinctive body odour (Spinney, 1994).

### KEYSTROKE DYNAMICS

Functionality

Keystroke dynamics is based on the concept that how a person types, in particular their rhythm, is distinctive. Keystroke dynamics are behavioural and evolve over time as users learn to type and develop their own unique typing pattern. The National Science Foundation and the National Bureau of Standards in the United States have conducted studies establishing that typing patterns are unique (Miller, 1987). The technique works best for users who can "touch type". The health and fatigue of users, however, can affect typing rhythm (Roethenbaugh, 1998b).

This technology has experienced a recent resurgence with the development of software to control computer and Internet access. One system creates individual profiles according to how users enter their passwords, accounting for factors such as hand size, typing speed, and how long keys are held down (Nelson, 1998). Reportedly, the technology can be used with any keypad, "from computer keyboards to automated teller machines to telephones" (Net Nanny, 1998). Previously, differences in keyboards had been one of the problems that had limited the implementation of keystroke dynamics.

### GAIT RECOGNITION

Functionality

Research in underway at several universities,[17] focusing on the automated recognition of people by their ***gait*** or specific perambulatory movement. When a person walks, body parts – the legs, knee joints, arms, elbows, and so on – create a particular repeating pattern as they each move through space. A video camera captures these points of movement and sends them to a computer for analysis. The computer notes the movements and establishes mathematical relationships for each point to create the "signature" patterns it needs to recognise for each individual.

DARPA funding from the US government is furthering this research in support of the "Human ID at a Distance" project.[18] "Unlike faces and irises, someone's gait can be spotted from a great distance with low-resolution cameras and so be observed from just about any angle. It is also very difficult to mask" (*New Scientist*, 1999). Obvious applications include the perimeter defence of embassies and military installations.

*Biometric summary table*

Table 1 sets out a general summary of some biometric-based technologies. The reader is cautioned that this table is very subjective and approximate in nature. The elements shown may be subject to high variability depending upon context, usage, algorithm, etc. Given that some biometric technologies are more mature than others and given that biometric systems are very contextually dependant, actual results will vary depending upon the technology selected, the intended application and the enrolled population size. Additionally factors such as acquisition and search time (which goes beyond the scope of this report) should also be used to properly interpret this summary table.

Table 1. **Biometric summary table**

| Biometric | Accuracy | Ease of use | User acceptance | Stability | Cost | Trans-parency[1] | Typical applications | Suitability for | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 1:1 | 1:N |
| **Finger-scanning** | High, possibly Very High | High | Medium Low | High | * to *** | Overt | Traveller clearance, driver's license, welfare | Yes | Yes |
| **Hand geometry** | High | High | Medium High | Medium High | *** | Overt | Access control, traveller clearance, day care | Yes | No |
| **Facial recognition** | Medium High[2] | Medium High | High | Medium Low | *** | Covert | Casino, traveller clearance | Yes | Poten-tially[3] |
| **Iris scanning** | Very High | Medium Low | Medium High | High | ***** | Covert | Prisons, access control, traveller clearance | Yes | Yes |
| **Retinal scanning** | Very High | Low | Low | High | **** | Overt | Access control, traveller clearance | Yes | Yes |
| **Finger geometry** | Medium | High | Medium High | Medium High | *** | Overt | Access control, amusement park ticket holder | Yes | No |
| **Voice recognition** | Medium | High | High | Medium Low | * | Covert | Low security applications, telephone authentication | Yes | No |
| **Signature verification** | Medium | High | Medium High | Medium Low | ** | Overt | Low security applications, applications with existing 'signature' | Yes | No |

*Notes:*

1. Transparency records the potential to which a system may be operated in a covert manner, without the knowledge of the individual to be identified. Overt systems require the knowledge of the data subject for biometric collection, covert systems do not.

2. Although the "potential" exists for high accuracy (as suggested in the controlled environment of the recent Facial Recognition Vendor Test (FRVT), recent pilot projects and real world tests have indicated much higher error rates and great difficulty in obtaining accurate results with these systems.

3. Ibid.

*Source*: Author.

### *Discussion*

A review of the publicly available biometric performance data and the media reports of biometric-based technology trials leave the reader with one conclusion: biometrics are not quite "ready for prime time yet". That is to say, while they appear to function adequately in small, limited 1:N identification implementations (and indeed in some larger 1:1 verification implementations), their accuracy, reliability and convenience are not yet sufficiently refined for very large population identification systems. Although media and anecdotal reports have provided an indication of possible success with respect to a number of larger implementations; third party performance data confirming the success and providing important contextual information about the implementation (performance, accuracy and exception processing) has not been so forthcoming.

This does not mean that we should eschew the technologies entirely. Indeed, when used properly biometric-based technologies allow us to solve novel problems and, in fact, enhance security ***and*** privacy. For example, a system designer can use biometric-based technologies to ensure the physical participation of an individual in an electronic transaction or face-to-face encounter. This type of design was recently considered in a project the author was involved with. Personal information was to be stored on a smart card to be carried by the data subject. Only the data subject's physical presence (confirmed by their biometric) would allow the smart card to "unlock" or allow a database update or access to take place. This type of strategic use of biometric-based technologies could provide defences against both identity theft (enhancing

security) and also against improper usage of back-end databases containing personal information (enhancing privacy).

A popular misconception held by the general public (and, unfortunately, by some vendors), is that an individual can be positively identified using a biometric-based system. We need to remember that all ***any*** system can do is to give a degree of correlation and (depending upon population size) with 1:N searching a number of candidate matches that exceed the match threshold.

A clear reminder about the limitations of the technology comes from Michael Thieme, Director of Special Projects at New York based International Biometric Group:

> "Face recognition expresses the PROBABILITY that two images are from the same person. Neither face recognition software, nor any other biometric, can make a definitive determination that any two people are "really" the same people …
>
> Turning to facial recognition, or any other biometric, to make a definitive determination is inconsistent with the basic precepts of biometric technology." (Thieme, 2003).

By preferring 1:1 authentication systems over 1:N identity systems, we can more easily control the error rate and performance of a given biometric-based technology and consequently, the likelihood for a successful implementation.

Recommendations

In general, a number of lessons may be learned from the existing biometric trials, pilot projects and system implementations. Within the constraints and specific limitations of any particular project, system designers and implementers should strive to:

- Communicate openly and honestly about any planned system.
- Ensure appropriate supervision of individuals interacting with biometric systems.
- Ensure appropriate fallback and exception processing procedures exist.
- Ensure that related functions (registration, program eligibility) support and enhance the security and privacy of a biometric system and do not present an opportunity, *e.g.* identity theft using a correct biometric.
- Initially, develop small and medium-sized, focused, inward-looking systems before considering large and very large population size systems. That way, performance problems become more manageable, lessons may be learned and improvements may be made as the technology matures.
- Consider the use of pilot systems and trials to allow biometric performance data to be gathered in real-world situations prior to large-scale system implementation.
- To minimise privacy impact and to increase biometric accuracy, focus on 1:1 authentication systems instead of 1:N identification systems.
- Ensure that a biometric-based technology is an appropriate solution to the problem being solved as opposed to the default authentication method. Ensure that user acceptance and cultural sensibilities are respected.
- Whenever possible, develop opt-in voluntary enrolment systems.
- Collect biometric samples openly and with the consent of the user.

- If possible, allow the user to retain custody of the biometric template (perhaps on a smart card or token) and ***do not*** store the biometric template in a central system.

Concerns

The author has identified the following concerns with biometric-based technologies:

- A biometric system may be improperly trusted to match or reject an individual. A system will generate errors and a system may have insufficient rigour in the enrolment phase to verify an individual's identity.
- There are limited sources of independent performance metrics.
- For very-large population biometric systems, all metrics are the result of extrapolation and consequently have large potential error factors.
- Care must be taken to avoid an 'underclass' of those unable to authenticate using biometric-based technologies due to failure-to-enrol and failure-to-acquire errors.
- Some vendors of biometric-based technologies may appear opportunistic in the presentation of their solutions post September 11th, 2001.
- Biometric-based solutions run the risk of becoming a technology panacea, the public tends to over-estimate their accuracy and capabilities and also may improperly associate the technology with protection from terrorism.
- The risk of a large-scale biometric system failure (a system having unacceptable performance which necessitates extensive exception processing) is high.

**Standards for biometrics**

To enhance interoperability between biometric systems, standards are being developed by different organisations.

- General biometric standards include:
  - The US National Institute for Standards and Technology (NIST) has defined CBEFF (Common Biometric Exchange File Format), a "common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange".[19]
  - The Organization for the Advancement of Structured Information Standards (OASIS) is working on XCBF (XML Common Biometric Format), an XML representation of the CBEFF patron formats.[20]
  - The BioAPI consortium works has defined an application programming interface (API) to facilitate the programmers' task when implementing software related to biometric systems.[21]
- The need for biometric standards in the travel area is being considered by ISO/IEC and ICAO:
  - ISO (International Organization for Standardization) / International Electrotechnical Subcommittee Joint Technical Committee (IEC JTC 1[22]) on Information Technology has:
    - Subcommittee 17 on cards and personal identification.[23]
    - Subcommittee 27 on security techniques.

- Subcommittee 37 on biometrics.[24] Of particular interest is the special group 6 dealing with societal and other issues related to biometrics (including privacy).

- ICAO Technical Advisory Group on Machine Readable Travel Documents (TAG/MRDT) has developed a revision of document 9303 to "provide for machine-assisted identity confirmation of the rightful holder of the MRTD". This revision includes a globally interoperable biometric in a machine readable travel document.[25]

***Privacy standards for biometrics***

While both ICAO and ISO have attempted to address the issue of privacy within the standards development context, their well-intentioned efforts have to some degree been unsuccessful in the opinion of the author. In large part, this may be due to the repeated presentation of privacy as a "public acceptance" issue instead of an objective systems design and governance issue. Public opinion and acceptance of an initiative may be useful in telling us when something is wrong, but public acceptance ***cannot*** address all of the privacy concerns of a proposed initiative or standard.

**Implementation methodologies and frameworks**

As indicated in the introduction of this report, it is hoped that a framework which supports the implementation of biometric-based technologies in a privacy-enhancing and security-enhancing manner may be developed from the discussions in this paper.

Below are presented a number of approaches to ensure that a given system complies with privacy and/or security requirements. These are provided for discussion purposes in the hope that they will stimulate further development.

***Existing privacy and security methodologies for biometrics***

*Statutory – using the law to protect security and privacy*

In some jurisdictions, generalised or specific criminal sanction may be used to provide security protection for biometric systems and to outlaw certain activities to bypass security controls.

A number of jurisdictions have also proposed or enacted specific legislation to afford privacy protection in the context of biometric usage. This may either replace or augment the use of general-purpose privacy legislation. Annex I contains two examples from North America.

*Policy – security and privacy compliance*

Policies and policy-based protections are commonly used to protect security and privacy.

The Privacy Impact Assessment (PIA) and privacy audits can ensure that privacy policies are followed and ensure that the policies meet the needs of a given level of privacy protection or compliance. Although these techniques are commonplace within government, they are just starting to appear in the private sector.

Security threat risk assessments and security audits have historically been used to ensure that security policies are followed and that they are appropriate.

The Common Criteria scheme is a flexible and formal framework that may be used to verify that a given computer system or product meets its stated security protection profile. Work is underway to adapt the common criteria scheme to allow for privacy protection profiles (Adams *et al.*, 2002).

*Technology – building security and privacy rules into the system*

**HARDWARE PROTECTIONS FOR SECURITY AND PRIVACY**

Tamper-proof hardware

Hardware protection is widely utilised and accepted to provide an enhanced level of security in many systems. It is commonplace in the banking industry to have specific hardware requirements for pin-pad and ATMs, and systems utilised for national security purposes almost always have self-destructing tamper-proof encryption devices (Schneier, 1996). As noted by one security expert, "Historically, NSA (the US National Security Agency) has refused to approve software based systems for encrypting classified information. It's just too easy to attack the software … and cause all sorts of hard to detect weaknesses in the crypto" (Smith, 1998).

This tamper-proof hardware is designed to ensure that a technician or programmer cannot ***easily*** and ***efficiently*** defeat the security protections in a given system.

A similar approach may be employed to protect privacy in biometric systems. In essence, by utilising specific hardware components, certain rules could be built into the biometric system.

These rules would represent specific privacy policies and rules for system operation.

Under such a system, there would be no way that a software designer could bypass the privacy policies. This would in effect imbue a piece of hardware with the "knowledge of good and evil" — the hardware would know when to allow the biometric system to function (by controlling the link to an identity for example) and when to disallow it. These tamper-proof pieces of hardware would utilise cryptographic primitives secured by hardware keys that would be unknown to the system designer or operator, or indeed, anyone else. (This may be accomplished using secured key injection modules escrowed with third parties.)

As noted above, a well-known model currently exists in the security world that performs in this very manner: ATMs and pin-pad devices have similar tamper-proof hardware components communicating with tamper-proof hardware attached to bank mainframe computers. The hardware "knows" when a transaction is legitimately initiated. The key is initially loaded into the tamper-proof hardware using secure key injection and may be re-injected again without the operator "knowing" what the key is.

One possible scenario in which this could be accomplished is through the use of trusted tokens — in effect, a small computer in a tamper proof box residing in the biometric scanner, with another trusted token residing in the central biometric server. These two pieces of hardware would "trust each other" and nothing else. The central token would refuse to divulge an identity unless the request had come from its partner within the scanner. This would prevent a biometric system from being used without the consent of the data subject (with, for example a latent fingerprint) (Borking, 1996).[26]

(Trusted tokens are general-purpose computers, which are easily configurable and securable. The logic, which requires the use of strong encryption and a request being initiated by the corresponding scanner, is 'burned into' the tokens. Any attempt to reprogram or reverse engineer the tokens will destroy them in the process.)

Identity protector

John Borking of the Dutch Protection Authority (*Registratiekamer*) has written extensively about the Identity Protector, a component than can increase privacy by restricting the flow of identity information within a complex system. This identity specific hardware component is similar to the abstract de-identification component of privacy architecture (see below).

### STEPS – SECURITY TECHNOLOGY ENABLING PRIVACY

Security Technology Enabling Privacy (STEPs) (Cavoukian, 2002) is an initiative of the Information and Privacy Commissioner/Ontario. As noted in their paper:

> "Historically, privacy and security have been treated as opposing forces in a zero-sum game. Such a view, by necessity, invokes a balancing act, where the greater the gains for one side, the greater the losses for the other. In a game theory paradigm, the more you have of one, the less you can have of the other, so that the sum always remains 'zero.' But this win/lose attitude poses a major threat for privacy, since the public's desire for safety and security is so high. Continuing the post 9/11 debate within this framework threatens the very foundation of privacy, leaving its future in question.
>
> This is why we must change the paradigm. This paper argues there is no inherent reason why greater safety and security must come at the expense of privacy. If we can reframe the issue, challenging the underlying premise - that we must cede privacy in order to gain security, then we can take the necessary steps to improve both. Many security technologies can be redesigned to remain highly effective, while at the same time, minimising or eliminating their privacy invasive features. If we substitute a new premise – that privacy and security are two complementary sides of an indivisible whole (not polar opposites), then we can design technologies that protect public safety without sacrificing privacy." (Cavoukian, 2002)

In addition to biometric encryption, the STEPs paper gives the following example of security technology enabling privacy:

> "Passenger scanning technologies are commonplace at all airports and are deployed to identify possible security threats. However, scanning technology has the potential to intrude on the physical privacy of the individuals being scanned. Researchers at the US Department of Energy have developed a new technology that augments security scanning while addressing this privacy concern. The Department's Pacific Northwest National Laboratory has produced a scanning technology, using 3-D holographic imaging, that focuses on revealing objects hidden underneath the clothing of airline passengers, instead of displaying the entire body. In addition to metal weapons, those made of plastic and ceramics can be detected by the Personal Security Scanner, thus offering a distinct advantage over surveillance systems that rely on metal detectors alone. The scanner uses non-harmful ultrahigh-frequency radio waves with relatively large wavelengths that can penetrate clothing. Concerns that the unclothed physical features of a person being scanned might be visible to the scanner operator were addressed by reprogramming the system to give the operator a view of only concealed items, and not the person's image. The Personal Security Scanner is an excellent example of technology that is designed and deployed in a manner that addresses security requirements while minimising the intrusion into personal privacy." (Cavoukian, 2002)

*Security and privacy architecture*

Security architecture

System developers frequently use a formal process known as a "security architecture" to ensure that security is built into a given system design. Security architecture is a formal design that builds on a threat risk assessment and security policy to produce a system design that mitigates risk and enhances overall system security.

At an atomic level, the building bricks of security architecture are authentication, access control, data confidentiality, data integrity and non-repudiation.[27]

Privacy architecture

A similar approach may be applied to privacy, and the development of a "privacy architecture" (Hope-Tindall, 2002b). Privacy architecture is a formal design process that builds on a privacy impact assessment and privacy policy to produce a system design which mitigates risk and enhances overall system privacy.

Privacy architecture usually considers various options or models for system design and after analysis selects the option or model which meets the business requirement with the least amount of "privacy impact". It is, of course, necessary to perform a privacy impact assessment in conjunction with and to facilitate the privacy architecture process.

Consistent with the collection limitation and data quality principles of the OECD Privacy Guidelines, the goal of a privacy architecture is to minimise the amount of identity in a transaction to the extent relevant to the purpose for which the personal data is collected. A privacy architecture combines technology, policy, oversight and governance into a single "system" design to protect and enhance informational privacy. Annex II provides a discussion of the building blocks of a privacy architecture and the positioning of privacy architecture in general.

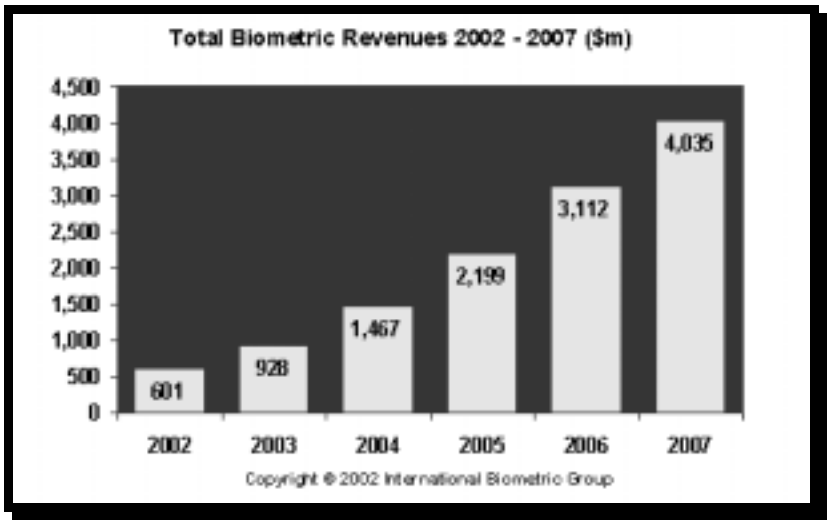
One essential design element (the physical location of the biometric template) could be addressed within an overall "privacy architecture". As an example, storing the biometric template on a smart card instead of in a centralised database may assuage many of the privacy concerns of biometric systems, as long as appropriate protections to secure the smart card and biometric system are taken (restricting access through authorised reader and PIN code, for instance). The smart card can travel with the data-subject, who can exercise the ultimate consent mechanism, physical custody of his own biometric. We see examples of this in the Schiphol frequent traveller system (CNN, 2000; Chua, 2001), and Bioscrypt, a Canadian company has started to market a product specifically to take advantage of this non-centralised architectural design (Smart Card Alliance, 2002). Further privacy enhancement can be derived from the strategic use of public key infrastructure (PKI), virtual private network (VPN) and other security technologies within a biometric system design.

**Biometric industry**

Even before the heightened interest in biometric technologies that followed the events of September 11th, 2001 the biometric industry had forecast significant revenue growth in the near future. This forecast has only expanded as vendors, governments and citizens have begun to think of biometric technologies as a general solution to the security problems faced by many countries and organisations.

According to the exhaustively complete and authoritative *Biometric Market Report 2003-2007*, available from the International Biometric Group, revenues are expected to reach over USD 4 billion by 2007, driven by large-scale public sector biometric deployments, the emergence of transactional revenue models, and the adoption and implementation of standardised biometric infrastructures and data formats (see Figure 7).

Figure 7. **Projected biometric market growth**




*Source*: IBG (2002), *IBG Biometric Market Report 2003-2007*.

Given the forecast expansion of the biometric market, and the financial performance of many biometric vendors, the author does not believe that the biometric industry requires further outside stimulation or development at this time to achieve significant growth. However, the success, usability and public acceptance of various biometric initiatives, and future improvements in the science of biometrics (system accuracy, performance, security and privacy) will require a combined effort on the part of vendors, customers, industry groups and even users of biometric systems.

Various industry groups and associations exist, some countries already have dedicated biometric management offices to co-ordinate the acquisition and implementation of biometric technologies within their national governments, some have also created testing and evaluation centres and initiatives to report on the effectiveness and usability of biometric technologies. The European Union also supports BIOVISION (a roadmap for Biometrics in Europe: 2003-10), a project which aims to contribute to a secure, user-friendly, socially acceptable and ethical use of biometrics in Europe.

While these developments are certainly worthwhile, the author believes that there is a place for some kind of "global" multinational biometric research initiative. This initiative could encourage further research into ethical identification and authentication technologies, and could develop and encourage models for such technologies for enhanced security, user-friendliness, technological transparency and respect for privacy. Additionally, this initiative could encourage an independent and transparent testing process for biometric technologies to ensure that vendors, customers and users have access to accurate, appropriate and "real-world" metrics of system performance.

The author also believes that it is necessary to educate system users and the public in general by dispelling some of the myths and misconceptions of biometric-based and DNA-based technologies. There is great need and tremendous opportunity for an international initiative in this specific area. Vendors and

customers also need to be educated in the ways of security and privacy so that they appreciate the potential benefits and the business imperative for doing so. Indeed, without this focus on security and privacy, concerns by end-users will likely limit the development of biometric-based technologies and the acceptance of their application. The future will only improve when we have an honest assessment of the *status quo*, the problems and opportunities of today and when we ***all*** work to encourage and develop the best technology for the future in the best way.

**Conclusion**

The time of biometric-based technologies is upon us. We need to understand their respective limitations, benefits and risks. We need to identify and classify potential uses to ensure that the technology is appropriate, suitable, cost-effective and accurate.

The extent to which we are willing to incorporate statutory ***and*** policy ***and*** technological controls into these systems and technologies will determine the extent to which they will improve our quality of life; providing convenience and security or conversely, the extent to which they threaten our liberty and freedom via actual or potential surveillance and control.

We should not have to choose between security and privacy. By acting responsibly, and with a lot of hard work, we can and ***must***, have both. To this end, is it imperative that we support and promote the development of security-enhancing and privacy-enhancing technologies, techniques and methodologies.

## NOTES

1. The phrase “right to be let alone” had been coined by Judge Cooley several years earlier (Cooley, 1888). .
2. National Standards of Canada Model Code for the Protection of Personal Information, CAN/CSA-Q830-96.
3. Schedule 1 - *Personal Information Protection and Electronic Documents Act* - Statutes of Canada 2000, c. 5, “PIPEDA”.
4. For more details, see also http://europa.eu.int/comm/justice_home/doc_centre/asylum/fingerprints/doc_asylum_fingerprints_en.htm and http://europa.eu.int/comm/justice_home/news/information_dossiers/news_eurodac_whatis_en.htm, both sites accessed 20 April 2004.
5. Market research method and system for collecting retail store and shopper market research data, Assignee: A. C. Nielsen Company, US Patent Number: 5331544, 19 July 1994.
6. For example, a hill-climbing attack.
7. See “The Facial Recognition Vendor Test – 2000” and “The Facial Recognition Vendor Test – 2002”, www.frvt.org, accessed 20 April 2004.
8 See “The Fingerprint Verification Competition – 2002”, http://bias.csr.unibo.it/fvc2002/, accessed 20 April 2004.
9. See http://infowar.net/tia/www.darpa.mil/iao/HID.htm, accessed 20 April 2004.
10. Refer to Note 4 above.
11. Following the events of September 11th, 2001.
12. Mayfair Lakeshore Racquet & Fitness Club. For more information, see www.cbc.ca/consumers/market/files/home/biometrics/dayinlife.html, accessed 20 April 2004.
13. See www.identix.com/newsroom/lfa.html, accessed 20 April 2004.
14. Refer to Note 13.
15. For example, see http://faculty.darden.virginia.edu/smithr/Biometrics.doc, accessed 20 April 2004.
16. For more information, see www.cbsa-asfc.gc.ca/travel/canpass/menu-e.html, accessed 20 April 2004.
17. For example, see www.isis.ecs.soton.ac.uk/image/biometrics/gait/, accessed 20 April 2004.
18. For more information, see www.gait.ecs.soton.ac.uk/, accessed 20 April 2004.
19. Founded in 1901, the NIST is a non-regulatory federal agency within the US Commerce Department’s Technology Administration. NIST’s mission is to develop and promote measurement, standards and technology to enhance productivity, facilitate trade, and improve the quality of life. For more information on CBEFF, see www.itl.nist.gov/div895/isis/bc/cbeff, accessed 20 April 2004.
20. OASIS was founded in 1993 under the name SGML Open as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the SGML (Standard Generalized Markup Language). The name OASIS was changed in 1998 to reflect an expanded scope of technical work, including the Extensible Markup Language (XML) and other related standards. For more information, see www.oasis-open.org/committees/tc_home.php?wg_abbrev=xcbf, accessed 20 April 2004.
21. The BioAPI Consortium was launched in April 1998 as a consortium grouping different players of the biometric field. See www.bioapi.org, accessed 20 April 2004.
22. For more information, see www.jtc1.org, accessed 20 April 2004.
23. See www.sc17.com (accessed 20 April 2004) for more information.
24. See www.jtc1.org/Navigation.asp?Mode=Browse&Area=Structure&SubComm=ISO%2FIECJTC1&CommLevel=TC&OldSubComm=ISO%2FIEC+JTC+1&SCCODE=, accessed 20 April 2004.
25. See www.icao.int/mrtd/publications/doc.cfm, accessed 20 April 2004.
26. Also see the articles in the *Schwerpunktheft ‘Digitales geld’, Datenschutz und Datensicherheit*, 7, 1997.
27. ISO7498-2 Security Architecture reference.

## REFERENCES

AcSys Biometrics Corp. and Nexus Group International Inc. (2001) "AcSys Biometrics Management Group Available For Comment", Media Advisory, 12 September, www2.cdn-news.com/scripts/ccn-release.pl?/2001/09/12/091201-7118-e.html, accessed 20 April 2004.

Adams, Dawn *et al*. (2002), "IBM Domus ITSL", presentation to the PETTEP Working Group at the 12th Conference on Computers, Freedom and Privacy, San Francisco, 16 April.

Association for Biometrics and International Computer Security Association (1998), "1998 Glossary of Biometric Terms", revised 1999 version available at www.afb.org.uk/docs/glossary.htm, accessed 20 April 2004.

Australian Justice and Customs (2002), "Passport Verification World First", 26 August, www.law.gov.au/www/justiceministerHome.nsf/Web+Pages/ED7C05CFE3763380CA256C220003EEEE?OpenDocument, accessed 20 April 2004.

Baker, Geoff (1997), "Newest Form of ATM Security Catches Eye of Banking Industry," *Ottawa Citizen*, 3 July, p. C1.

Belsize, Laurent (1997) "Coming Soon: ATMs That Recognise Your Eyes", *Christian Science Monitor*, 2 December.

Biome Partners, Inc. (1999), "New 3D Finger Geometry Biometrics for OEM's and Systems Integrators", Press Release, 15 January.

*Biometric Digest* (1998), "Mr. Payroll Corp.'s Machine Makes Military Base Debut", June, p. 3, www.biodigest.com/BiometricDigest/BackIssues/199806.pdf, accessed 20 April 2004.

*Biometric Technology Today* (1998), Vol. 6, No. 5, September, pp. 6, 8.

Bonier, Paul (n.d.), "Up Close and Personal: Biometrically Identifying Bank Customers Eye to Eye is an Invasion of Privacy," *Kitchener-Waterloo Record*, p. A11.

Bonsor, Kevin (n.d.), "How Facial Recognition Systems Work", http://computer.howstuffworks.com/facial-recognition.htm/printable, accessed 20 April 2004.

Borking, John, (1996) "Der Identity Protector" and "Einsatz datenschutzfreundlicher technologien in der Praxis", *Datenschutz und Datensicherheit*, 11, pp. 636-640; 654-658.

Burnell, John (1997), "Identifying the Biometric Opportunity: Biometric Technology is Now an Affordable Tool for Many Users and Applications Beyond Security", *Automatic ID News*.

*Business Week* (2002), "Why Visionics Is Flying Higher", 14 January, www.businessweek.com/magazine/content/02_02/c3765101.htm#B3765105, accessed 20 April 2004.

Cavoukian, Ann (2002), "Security Technology Enabling Privacy (STEPs): Time for a Paradigm Shift", Information and Privacy Commissioner/Ontario, June, www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13289&N_ID=1&PT_ID=11351&U_ID=0, accessed 20 April 2004.

Chua, June (2001), "Biometrics: The Future of Security", *CBC News Online*, September, www.cbc.ca/news/indepth/background/wtc_biometrics.html, accessed 20 April 2004.

Cilluffo, Frank J. (2000) "Cyber Attack: The National Protection Plan and its Privacy Implications", statement by Mr. Cilluffo, Deputy Director, Organised Crime Project Director, Task Force on Information Warfare and Information Assurance, Center for Strategic and International Studies to the United States Senate, 1 February.

Clarke, Roger (2003), "SmartGate: A Face Recognition Trial at Sydney Airport", Australian National University, Department of Computer Science, 26 August, updated 7 February 2004, www.anu.edu.au/people/Roger.Clarke/DV/SmartGate.html, accessed 20 April 2004.

CNN (Cable News Network) (2000), "Schipol Backs Eye Scan Security", CNN.com/WORLD, 27 March, www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/, accessed 20 April 2004.

Cole, George (1995), "Giving Voice to Security" *Financial Times*, 15 September.

Cooley, Thomas M. (1888), *Cooley on Torts 29*, 2nd edition.

Curran, John (2001), "Casinos Using Facial Surveillance", Associated Press, 26 February, www.crimelynx.com/casino.html, accessed 20 April 2004.

Delaney, Kevin and Paulo Prada (2002), "In Security, the Eyes Tell All: IBM and Dutch Airport to Sell State-of-the-Art Iris-Scanning System", *Wall Street Journal Europe*, 28 April, www.biometricgroup.com/in_the_news/wsj_europe.html, accessed 20 April 2004.

EC (European Commission), (2003), "European Fingerprint ID System Will Track Asylum Seekers", Press Release, The European Commission: Representation in the United Kingdom, 14 January, www.cec.org.uk/press/pr/pr03/pr0302.htm, accessed 20 April 2004.

*eSchool News* (2000), ""Best Practices – Technology: This Minnesota High School Gives Fingerprint Scanning a Whorl"", *eSchool News Online*, 1 September, www.eschoolnews.com/news/showStory.cfm?ArticleID=1277, accessed 20 April 2004.

*eSchool News* (2001), "Fingerprint Technology Speeds School Lunch Lines", *eSchool News Online*, 29 January, www.eschoolnews.com/news/showStory.cfm?ArticleID=2146, accessed 20 April 2004.

findBIOMETRICS.com (n.d.), "Hand Geometry – Now and in the Future", www.findbiometrics.com/Pages/hand_finger%20articles/hand_2.html, accessed 20 April 2004.

Fonseca, Brian (2002), "Airports Look to Biometrics for Security: Integrated Facial Recognition, Digitally Protected Passports on the Way", *InfoWorld*, 1 March, www.infoworld.com/article/02/03/01/020301hnbiometrics_1.html, accessed 20 April 2004.

Golgotha, Guy (1999), "Bar Codes for the Body Make it to the Market: Biometrics May Alter Consumer Landscape", *Washington Post*, 21 June, p. A1.

Hamilton, Tyler (2003), "Finger on the Future", *The Toronto Star*, 17 May.

Holmes, J., L. Wright and R. Maxwell (1991), "A Performance Evaluation of Biometric Identification Devices", Sandia Report, Sandia National Laboratories, SAND91-0276/UC-906, June, http://infoserve.sandia.gov/cgi-bin/techlib/access-control.pl/1991/910276.pdf, accessed 20 April 2004.

Hope-Tindall, Peter (2002a), "Privacy Impact Assessment – Obligation or Opportunity: The Choice is Ours!", paper presented at the CSE ITS Conference, Ottawa, Ontario, 16 May, www.enterpriseprivacy.com/cseits2002/ITS%20Material.pdf, accessed 20 April 2004 (also attached to the present report as Annex II).

Hope-Tindall, Peter (2002b), "Privacy Architecture", presentation to Showcase Ontario 2002, 10 September, www.enterpriseprivacy.com/Corp2002/2000-09-10Arch_files/frame.htm, accessed 20 April 2004.

IBG (International Biometric Group) (n.d.a), "How is 'Biometrics' Defined?" www.biometricgroup.com/reports/ public/reports/biometric_definition.html, accessed 20 April 2004.

ICAO (2003b), "Biometric Deployment of Machine Readable Travel Documents", ICAO TAG MRTD/NTWG Technical Report, Version 1.9, 19 May, www.icao.int/mrtd/download/documents/ Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents.pdf, accessed 20 April 2004.

ICAO (International Civil Aviation Organization), (2003a), "ICAO Recommendation", www.icao.int/mrtd/biometrics/recommendation.cfm, accessed 20 April 2004.

IR Recognition Systems (1998), "A Show of Hands Keeps School Children Safe," Press Release, 16 November, www.handreader.com/news/pressreleases/1998_archives/981116.htm, accessed 20 April 2004.

Iridian Technologies, Inc. (n.d.), "Spring Technologies and Johan Rhea Tae Kwon Do Launch New Technology that Enhances Customer Service," Press Release (for more information on Iridian, see www.iriscan.com, accessed 20 April 2004).

Jackson, William (1997), "Digital Video Patrols Border: INS Inspectors in Montana Use Surveillance Equipment at Canadian Line, *Government Computer News*, 15 December, www.gcn.com/archives/ gcn/1997/December15/comm.htm, accessed 20 April 2004.

James, Frank (1997), "Body Scans Could Make ID Process Truly Personal", *Chicago Tribune*, 4 June, as cited in John D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?", Proceedings of the IEEE, Vol. 85. No. 9, September, p. 1483.

Lack, Bob (1999), "Development of Facial Recognition Technologies in CCTV Systems," *SourceUK.net*, 25 October, www.sourceuk.net/indexf.html?00624, accessed 20 April 2004.

Mansfield, T. *et al.* (2001), "Biometric Product Testing Final Report", CESG report, 19 March, www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf, accessed 20 April 2004.

Matsumoto, T. *et al.* (2002), "Impact of Artificial Gummy Fingers on Fingerprint Systems", Proceedings of the International Society for Optical Engineering, *Optical Security and Counterfeit Deterrence Techniques IV*, Vol. 4677.

McMilan, Robert (2002), "The Myth of Airport Biometrics", *Wired News*, 9 August, www.wired.com/news/conflict/0,2100,54418,00.html?tw=wn_story_related, accessed 20 April 2004.

McMurchie, Laura Lyne (1999), "Identifying Risks in Biometrics Use", *Computing Canada*, 12 February, p. 12, www.findarticles.com/cf_dls/m0CGC/6_25/53880053/p1/article.jhtml, accessed 20 April 2004.

*Mercury News* (1999), "Bank Will ID its Customers by Pattern of Eye's Iris," 13 May.

Miller, Benjamin L. (1987), "Biometrics: Getting Computers to Identify People," *Canadian Datasystems*, Vol. 19, No. 11, November, p. 65.

Milroy, Susannah (1998), "Biometric Identification and Access Control Go Hand-In- Hand", *SP&I News*, April.

MIT (Massachusetts Institute of Technology) (2002), "Photobook/Eigenfaces Demo", http://vismod.media.mit.edu/vismod/demos/facerec/basic.html, accessed 20 April 2004.

Miyake, Kuriko (2002), "Japan to Test Biometrics for Airport Check-in", IDG News Service, Tokyo Bureau, 6 November, security.itworld.com/4360/021106japanbio/page_1.html, accessed 20 April 2004.

Nelson, Matthew (1998), "Net Nanny Finds New Keys to Security: Let Your Fingers Do the Walking to a New Form of Password Protection", *InfoWorld Electric*, 9 October, www.pcworld.com/news/article/0,aid,8361,00.asp, accessed 20 April 2004.

Net Nanny (1998), "Net Nanny Releases Much Anticipated Alpha Version of BioPassword®, its Patented Keystroke Dynamics Security Solution", Press Release, 26 August, www.netnanny.com/press/press_980826.htm, accessed 20 April 2004.

*New Scientist* (1999), "Tripped Up: Watch How You Walk, You May Incriminate Yourself", 4 December.

O'Connor, Sean (1998) "Collected, Tagged, and Archived: Legal Issues in the Burgeoning Use of Biometrics for Personal Identification", *Stanford Technology Law Review*, STLR Working Paper, http://stlr.stanford.edu/stlr/Working_Papers/98_O_Connor_1/index.htm, accessed 20 April 2004.

OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris, www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html, accessed 20 April 2004.

OECD (Organisation for Economic Co-operation and Development) (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 1980, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, accessed 20 April 2004.

Pigg, Susan (2002), "Iris-Recognition Device to be Demonstrated: Technology Could Speed Path of Frequent Fliers", *The Toronto Star*, 24 September, www.hope-tindall.com/peter/2002_sep_24.htm, accessed 20 April 2004.

PR Newswire (1999a), "SAFLINK Develops Way to Secure Internet Banking/Brokerage Account Balances, Bill Payment, and Funds Transfer Using Biometrics", 24 June, www.findarticles.com/cf_dls/m4PRN/1999_June_24/54981904/p1/article.jhtml, accessed 20 April 2004.

PR Newswire (1999b), "Home Shopping Network and SAFLINK Corporation Ship Biometric Security to 5,000 Families", 11 May, http://www.findarticles.com/cf_dls/m4PRN/1999_May_11/54597538/p1/article.jhtml, accessed 20 April 2004.

Roethenbaugh, Gary (1998a), "An Introduction to Biometrics and General History", *Biometrics Explained*, Section 1.

Roethenbaugh, Gary (1998b), "Technology Overview", *Biometrics Explained*, Section 3.

Roethenbaugh, Gary (1999), "Types of Biometric", *ICSA Biometrics Buyer's Guide*, Chapter 4.

Rosen, Jerome (1990), "Biometric Systems Open the Door", *Mechanical Engineering*, Vol. 112, No. 11, November, p. 59.

RYCOM Inc. (n.d.), "Frequently Asked Questions (FAQs) About Iris Recognition", www.rycom.ca/solutions/security/iridian/media_faq.htm#9, accessed 20 April 2004.

Schneier, Bruce (1996), *Applied Cryptography*, John Wiley & Sons, Inc., pp. 223-224.

Smart Card Alliance (2002), "Bioscrypt On Board with HID's iCLASS(TM) for Access Control", Industry News, 14 May, www.smartcardalliance.org/industry_news/industry_news_item.cfm?itemID=346, accessed 20 April 2004.

Smith, Rick (1998), "Re: military encryption ?", Usenet posting to comp.security.misc, Secure Computing Corporation, 20 October 2004, http://groups.google.com/groups?oi=djq&selm=an_403329809, accessed 20 April 2004.

Soutar, Colin (n.d.), "Biometric System Security", Bioscrypt Inc., www.bioscrypt.com/assets/security_soutar.pdf, accessed 20 April 2004.

Spinney, Laura (1994), "Crooks Smelly Armpits Give the Game Away", *New Scientist*, 14 September, p. 10.

Thalheim, Lisa, Jan Krissler, and Peter-Michael Ziegler (2002), "Body Check: Biometric Access Protection Devices and their Programs Put to the Test", *c't*, www.heise.de/ct/english/02/11/114/, accessed 20 April 2004.

*The Toronto Star* (1995), "Pinched by the Ear", 6 July, p. 43.

Thieme, Michael (2003), "Was It Really Saddam on TV Last Night?", posting to The Biometric Consortium's Discussion List BIOMETRICS@PEACH.EASE.LSOFT.COM, 20 March.

Tomko, George (1996), "Biometric Encryption – New Developments in Biometrics", presentation at the 18th International Privacy and Data Conference, Ottawa, 19 September, www.privcom.gc.ca/speech/archive/02_05_a_960918_01_e.asp, accessed 20 April 2004.

Tomko, George (2002), "The Fundamental Problem with Template-based Biometrics", presentation at the 12th Conference on Computers, Freedom and Privacy, San Francisco, 16 April.

Townsend, Mark and Paul Harris (2003), "Security Role for Traffic Cameras", *The Observer*, 9 February, http://observer.guardian.co.uk/politics/story/0,6903,892001,00.html, accessed 20 April 2004.

US Department of State, "Enhanced Border Security and Visa Entry Reform Act: Questions and Answers", Office of the Spokesman, 9 May, www.state.gov/r/pa/prs/ps/2002/10049.htm, accessed 20 April 2004.

US House of Representatives (2002), "Enhanced Border Security and Visa Entry Reform Act of 2002", United States H.R. 3525, www.unitedstatesvisas.gov/pdfs/Enhanced_Border_SecurityandVisa_Entry.pdf, accessed 20 April 2004.

Warren and Brandeis (1890), "The Right to Privacy", 4 *Harvard Law Review* 4, 193.

Wayman, J. (2002), "Biometric Authentication Technologies: Hype Meets the Test Results", presentation made at the 11the USENIX Security Symposium, San Francisco, 5-9 August, www.usenix.org/events/sec02/wayman.pdf, accessed 20 April 2004.

Williams, Martyn (2002), "OECD Publishes Cybersecurity Guidelines", *ComputerWorld*, IDG News Service, 8 August, www.computerworld.com/governmenttopics/government/policy/story/0,10801,73297,00.html, accessed 20 April 2004.

Zunkel, Richard (1994), "Palm Reading for Protection," *Security Management*, November, pp. 89-90.

## ANNEX I – STATUTORY PRIVACY PROTECTION FOR BIOMETRICS

### Ontario Works Act - Statures of Ontario 1997, c. 25[1]

"Biometric information" means information derived from an individual's unique characteristics but does not include a photographic or signature image; ("*renseignements biométriques*").

Biometric information

75. (1) Where this Act or the regulations authorise a person to collect or use personal information, biometric information may be collected or used only for the following purposes:

1. To ensure that an individual is registered only once as an applicant, recipient, spouse, same-sex partner or dependent adult.

2. To authenticate the identity of an individual who claims to be entitled to assistance.

3. To enable an individual to receive and give receipt for assistance provided through a financial institution or other authorised provider.

4. To enable an applicant, recipient, spouse, same-sex partner or dependent adult to access personal information.

5. To enable an individual to make a declaration electronically by voice or other means for any purposes authorised under this Act.

6. To match data in accordance with an agreement made under section 71 or 72 for the purpose of ensuring eligibility for assistance or benefits. 1997, c. 25, Sched. A, s. 75 (1); 1999, c. 6, s. 50 (7).

(2) Biometric information may be collected under this Act only from the individual to whom it relates, in accordance with an agreement referred to in paragraph 6 of subsection (1) or in accordance with section 73.

(3) Biometric information shall not be disclosed to a third party except in accordance with,

(a) a court order or a warrant;

(b) an agreement under section 71 or 72 that is made for the purpose of ensuring eligibility for a social benefit program, including a social benefit program under the Income Tax Act or the Income Tax Act (Canada); or

(c) section 73.

(4) Biometric information to be collected from the individual to whom it relates shall be collected openly and directly from the individual.

1. www.e-laws.gov.on.ca/DBLaws/Statutes/English/97o25a_e.htm, accessed 20 April 2004.

(5) An administrator shall ensure that biometric information can be accessed and used only by those persons who need the information in order to perform their duties under this Act and that it is not used as a unique file identifier or common personal file identifier, except as authorised under subsection (1).

(6) An administrator shall ensure that biometric information collected under this Act is encrypted forthwith after collection, that the original biometric information is destroyed after encryption and that the encrypted biometric information is stored or transmitted only in encrypted form and destroyed in the prescribed manner.

(7) Neither the Director nor an administrator shall implement a system that can reconstruct or retain the original biometric sample from encrypted biometric information or that can compare it to a copy or reproduction of biometric information not obtained directly from the individual.

(8) The only personal information that may be retained together with biometric information concerning an individual is the individual's name, address, date of birth and sex.

(9) For the purpose of section 67 of the Freedom of Information and Protection of Privacy Act and section 53 of the Municipal Freedom of Information and Protection of Privacy Act, subsection (3) is a confidentiality provision that prevails over those Acts. 1997, c. 25, Sched. A, s. 75 (2-9).

**Biometric Identifier Privacy Act – State of New Jersey**[1]

**ASSEMBLY, No. 2448**
**STATE OF NEW JERSEY**
**210th LEGISLATURE**

INTRODUCED JUNE 13, 2002

**Sponsored by:**
**Assemblywoman JOAN M. QUIGLEY**
**District 32 (Bergen and Hudson)**

**An Act** concerning biometric identifiers and supplementing Title 2A of the New Jersey Statutes.

**Be It Enacted** *by the Senate and General Assembly of the State of New Jersey:*

1. This act shall be known and may be cited as the "Biometric Identifier Privacy Act."

2. As used in this act:

   "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of a hand or a face geometry.

   "Governmental entity" means the State, any agency, authority, or employee thereof, or any political subdivision of the State, including but not limited to any county, municipality, or school district, or any agency, authority, or employee thereof.

3. a. Notwithstanding any other provision of law to the contrary, no person shall obtain a biometric identifier of an individual, for the purpose of commercial advantage, without authorisation of the individual.

   b. A person who possesses a biometric identifier of an individual shall not sell, lease, or otherwise disclose the biometric identifier to another person unless:

   (1) The individual consents to the sale, lease or disclosure.

   (2) The sale, lease or disclosure completes a financial transaction requested or authorised by the individual.

   (3) The sale, lease or disclosure is required or permitted by federal or State law. Or

   (4) The sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose.

   c. A person who possesses a biometric identifier of an individual shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects other confidential information.

1. www.njleg.state.nj.us/2002/Bills/A2500/2448_I1.HTM, accessed 20 April 2004.

d. A person aggrieved by a violation of this section may bring an action in the Superior Court to enjoin further violation and to recover for the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.

e. Any person who violates any provision of this section shall be liable for a civil penalty of not more than USD 25,000 for each violation. Any such penalty shall be enforced and collected in accordance with "The Penalty Enforcement Law of 1999," P.L.1999, c.274 (C.2A:58-10 et seq.). Any action to collect or enforce any such penalty shall be brought in the Superior Court by the Attorney General or county prosecutor.

4. a. A governmental entity that possesses a biometric identifier of an individual shall not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(1) The individual consents to the sale, lease or disclosure.

(2) The sale, lease or disclosure is required or permitted by a federal or State law. Or

(3) The sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose.

b. A governmental entity that possesses a biometric identifier of an individual shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental entity stores, transmits, and protects other confidential information.

c. A governmental entity that possesses a biometric identifier of an individual shall establish a reasonable procedure under which an individual is entitled to have the governmental entity correct information about the individual that is possessed by the governmental entity and that is incorrect. The procedure shall not unduly burden an individual using the procedure.

d. A person aggrieved by a violation of this section may bring an action in the Superior Court, to enjoin further violation and to recover the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.

e. Information compiled pursuant to this section shall not be subject to disclosure pursuant to P.L.1963, c. 73 (C.47:1A-1 et seq.) as amended and supplemented.

5. This act shall take effect immediately.

STATEMENT

This bill, the "Biometric Identifier Privacy Act," provides guidelines for the use and distribution of biometric identifiers and establishes civil penalties for the misuse of the information.

A biometric identifier is a retina or iris scan, fingerprint, voiceprint, or record of a hand or a face geometry. Biometrics technology is a non-invasive method of using computer technology to provide automatic identification or identity verification or authentication of individuals. The technology acquires an image of a physical feature which is then applied to the algorithm to produce a "template." This "template" is then encrypted for data transmission and storage. This stored "template" can then be stored and compared against the live "template" when necessary. This technology is being used for criminal identification as well as in airport security systems, border clearances and for transaction verifications in internet businesses. It is the sponsor's intent to protect the users of this technology by insuring that this data is not obtained, disclosed, misused or released without an individual's authorisation.

Under the provisions of the bill a person cannot obtain another individual's biometric identifier information, for the purpose of commercial advantage, without authorisation from that individual. The bill prohibits a person who possesses a biometric identifier of another individual from selling, leasing, or otherwise disclosing this information unless: the individual consents to the sale, lease or disclosure; the sale, lease or disclosure completes a financial transaction requested or authorised by the individual; the sale, lease or disclosure is required or permitted by federal or State law; or the sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose. A person who possesses a biometric identifier of an individual would be required to store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which that person stores, transmits, and protects other confidential information. The bill provides that any person who violates the provisions of the act would be liable for a civil penalty of not more than $25,000 for each violation. The Attorney General or county prosecutor would bring the action to collect or enforce the penalty in Superior Court. Furthermore, the bill provides that any person who has been aggrieved by a violation of the act may bring an action in the Superior Court, to enjoin further violation and to recover the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.

In addition, the bill prohibits any governmental entity which possesses a biometric identifier of an individual from selling, leasing, or otherwise disclosing the biometric identifier to another person unless: the individual consents to the sale, lease or disclosure; the sale, lease or disclosure is required or permitted by a federal or State law; or the sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose. A governmental entity that possesses a biometric identifier of an individual would be required to store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental entity stores, transmits, and protects its other confidential information. The bill also requires the governmental entity to establish a reasonable procedure under which an individual is entitled to have the governmental entity correct information about the individual that is possessed by the governmental entity and that is incorrect. The procedure cannot be unduly burdensome.

## ANNEX II – PRIVACY ARCHITECTURE AND THE PIA

### Privacy Impact Assessment – Obligation or Opportunity: The Choice is Ours!

Peter Hope-Tindall


Prepared for CSE ITS Conference – Ottawa, Ontario – May 16th, 2002

The Privacy Impact Assessment (PIA) has become the favoured tool for the identification of privacy risks in proposed government and private sector initiatives. Indeed, in Canada, federal and provincial funding requirements mandate the production of some form of a PIA before work begins on a new technology, program or initiative. This has, unfortunately, reinforced a 'compliance mentality' view of the PIA as yet another hurdle to be overcome in the already cumbersome project and funding process.

Usually, at the funding submission or project approval stage, work has not progressed beyond the contextual and conceptual layers of system design, and in some cases certain elements in the contextual and conceptual layers will remain incomplete or subject to change.

The risk associated with producing a thorough PIA at project initiation time, is that the further down the design layers we travel (i.e. the closer to implementation) the less relevant the PIA may become; in fact, once enumerated in the PIA, risk factors may be thought of as 'documented and dealt with' even though an obvious correction or change exists either in policy or within a specific architecture layer which could mitigate the problem.

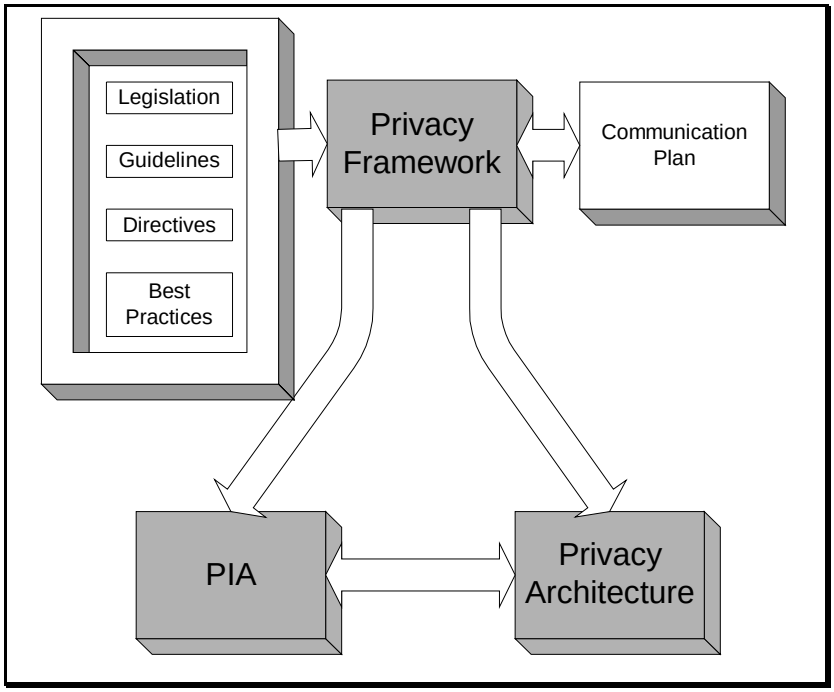
There is a substantial risk that a PIA may become an apology for the privacy shortcomings of a contemplated system and not an article for correction and change of the identified problems.

While it is important to document and evidence the due diligence in support of the quest for privacy, all too often, the main purpose of the PIA is to communicate the privacy risks to other parties (frequently, ***only*** the Privacy Commissioner) and to sit on a shelf gathering dust; a paperweight in which we can take solace – knowing that we have complied with the requirement to produce a PIA.

The author believes that another model exists, one in which the PIA can attain its lofty goals, one in which the PIA can be transformed from an apology into an authoritative text, from an obligation into an opportunity.

The author proposes a privacy triumvirate, a three-headed creature that addresses legislation, policy and technology. These components are 'Privacy Framework', our old friend the Privacy Impact Assessment 'PIA' and 'Privacy Architecture'.

Figure 1. **The 'three-headed privacy creature'**




**The Privacy Framework** contains many of the introductory and general provisions that appear in a traditional PIA. Usually, the context and metrics used for a traditional PIA are somewhat abstract. They consist of legislation, guidelines and directives, and in the case of the private sector, corporate policies and mission statements. It is simplistic and ineffective to suggest that a common application and equal weighting of these metrics will fit all new technologies, programs or services. This approach is somewhat arbitrary in that it is a measurement 'in a vacuum' against the same standard for all projects.

Instead, the author believes that these inputs should be used to synthesise a unique 'Privacy Framework' from among these various privacy imperatives. The customised Framework will allow the PIA and the Privacy Architecture to emphasise the important over the less important, to allow measurements and decisions to be made in the proper context and to facilitate solutions to problems instead of focusing on merely documenting issues.

The Privacy Framework allows for a customisation of the privacy drivers, tailored to fit the risk profile and specifics of a given project. This recognises that while for many projects the drivers will be identical (and by no means are we advocating an opportunistic 'situational ethics' view of privacy; moving the goal posts so the team can score) in some cases unique features of the program or technology will raise unique issues. Examples such as smart cards and projects utilising biometrics easily come to mind.

Best practices from other jurisdictions and an environmental scan of technology issues or solutions related to the initiative can be placed in the Privacy Framework, a placeholder for reference material for the steps below.

If properly constructed the Privacy Framework will serve as a kind of 'Privacy Constitution' for the PIA and Privacy Architecture, it will justify them and serve as an introduction to both of these other components. An additional benefit is realised, in that a comprehensive document is available for early submission with project funding requests and approval; and for early review by the Privacy Commissioner or oversight body. The importance of this demonstration of early good faith should not be underestimated.

Once the Privacy Framework has been crafted, it can be used to deliver consistent messaging and communications to all stakeholder groups, ***not just the Privacy Commissioner***. It can clearly communicate the privacy priorities and emphasis that a government or institution places on a given initiative. In many cases, it is this lack of effective communication that ultimately dooms a project in the face of a cynical public or vocal opposition from opposition groups.

**The PIA** allows us to fully explore the policy and non-technical elements of a proposed system as well as document the impact of technical design elements woven into the Privacy Architecture. The component contains the bulk of what most could consider a traditional PIA; a detailed review of the proposed system or project and a data flow and an impact analysis. Operating in support of the Privacy Framework it responds with policy changes; administrative controls; and recommendations for new legislation and directives. Many issues which are identified will be handed to the Privacy Architecture for solution.

It is important that the PIA be both active and responsive. Active in that opportunities for the introduction of privacy enhancing policies (which will tend to introduce elements of consent and individual control) are sought out; responsive in that compensating policy and legislative changes are introduced in response to issues raised during design, from the Privacy Architecture, and from difficulties encountered during implementation.

**The Privacy Architecture** allows us to truly build 'privacy into the design'. Operating in support of the Privacy Framework (as does the PIA) it responds with architecture improvements instead of policy changes; with technological controls instead of administrative controls; with hardware instead of laws and directives.

At the appropriate stage, as an addition to the communication plan, the Privacy Architecture allows us to communicate to external privacy stakeholder groups (*e.g.* the Privacy Commissioner, oversight and certification bodies) examples of our focus on the importance of privacy at the design stage.

More importantly however, the bringing together of all technical privacy components in a single book within the Privacy Architecture is an opportunity to allow technical problems identified in the PIA to be overcome and to allow technical problems identified in other architecture areas (Security, Network, Application, Technical) to be overcome. There may also be policy or other issues identified within the Privacy Architecture that will be passed back to the PIA for a policy or other non-technical solution.

It is important that the Privacy Architecture be both active and responsive. Active in that opportunities for the introduction of privacy enhancing components (which will tend to introduce elements of consent and individual control) are sought out; responsive in that compensating technical components are introduced in response to issues raised during design, from the PIA, and from fundamental policy decisions.

The reader should be cautioned that the PIA and Privacy Architecture will never be 'fully completed'. They will approach completion as the project is implemented, but the necessary steps of follow-up review and audit will remain ongoing for the duration of the project or system lifetime. Indeed, it is not uncommon for privacy issues in system design and policy review to arise only ***after*** a live system is up and running; the privacy regime employed ***must*** be flexible enough to allow a response in this situation.

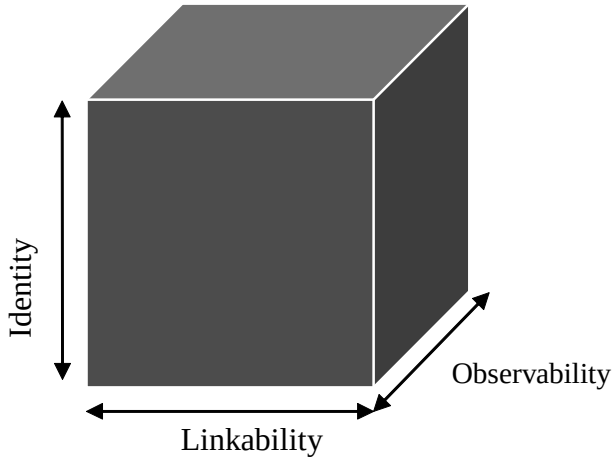
Metrics – How do we measure success?

With the PIA and the Privacy Architecture focused on finding solutions instead of documenting issues, we must now be able to measure the privacy impact of each possible solution somewhat objectively; to allow us to choose one solution over another.

The author proposes a three dimensional privacy metric to allow this measurement to be made somewhat, although not completely objectively.

The three dimensions are Identity, Linkability and Observability:

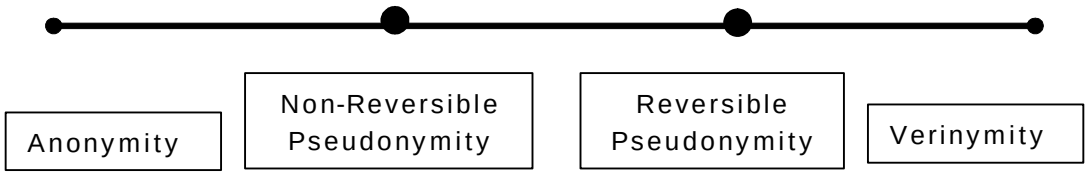
Figure 2. **Three dimensions privacy measurement**




**Identity (or nymity)**

Measures the degree to which information is personally identifiable.
The Identity measurement takes place on a continuum, from full anonymity (the state of being without name) to full verinymity (being truly named).

Figure 3. **Identity measurement**



The goal of the Privacy Architect and the PIA author is always to decrease the amounts of identity in a given system. A minimalist design approach should be employed and if identity data is not required, it should be intentionally removed from the architectural equation. Many tools employing reversible and non-reversible pseudonymity are available for this purpose. These identity tools are among the primary tools used by the workmen and workwomen known as 'Privacy Architects'.

**Linkability**

Measures the degree to which data elements are linked to each other. (Identity measurement can be thought of as the degree to which data elements are linkable to the verinym or true name of the data subject).

The requirements for unlinkability are intended to protect the user against the use of profiling of operations. For example, when a telephone smart card is employed with a unique number, the telephone company can determine the behavior of the user of this telephone card. Hiding the relationship between different invocations of a service or access of a resource will prevent this kind of information gathering.

Unlinkability requires that different operations cannot be related. This relationship can take several forms. For example, the user associated with the operation, or the terminal which initiated the action, or the time the action was executed.

The primary solution to linkability is generally the token-based approach, with an awareness of other factors [(time, location, message contents (which we refer to as observability)] which could also tend to allow transactions to be linked. In addition, approaches such as message padding and 'salting' are employed to prevent data matches.

**Observability:**

Measures the degree to which identity or linkability may be impacted from the use of a system.

These three metrics cannot provide an abstract measurement (unless some external reference standard is developed) however; they allow us to make a relative measurement comparing one solution to another. In all cases, the goal for the Privacy Architect and the PIA author is to minimise identity, minimise linkability and minimise observability.

While no system design or project implementation can be perfect, we believe that a balanced approach such as that advocated above will allow a government or institution to not only realise the best, most privacy protective solution for their proposed system; but will easily ***demonstrate*** that they delivered the ***very best possible*** solution.

Our approach of emphasising solutions over issues, while accepting that some issues may unfortunately remain unresolved, is clearly preferred to a process that simply documents and leaves all issues unresolved.

The key to a successful and privacy enhancing implementation is the recognition that three crucial areas need to be addressed; legislation, policy and technology.

# ANNEX III – DNA-BASED TECHNOLOGIES

## DNA

### *DNA identification*

DNA or deoxyribonucleic acid, is perhaps thought of as the ultimate identifier. At the heart of DNA identification is the human genome itself. Each person carries a unique genetic code, a sequence of over 3 billion nucleic acid base pairs – adenine (A), cytosine (C), guanine (G), and thymidine (T).

Every cell of a human body contains its own copy of that person's complete genetic code, determined at conception – a code that is different for every person on the planet, (with the exception of identical twins). Unlike fingerprints, there's no way to change a person's DNA by surgery or by cutting off the person's hands.

Today, this testing has three primary uses:

- Paternity and sibling testing (verification of genetic provenance).
- Identification of blood, semen and tissue samples left at crime scenes.
- Identification of human remains.

Yet, while DNA identification appears powerful, and in fact is very effective at ***excluding*** an individual from a given match, the system suffers from a fundamental flaw. The problem is that, unlike fingerprints, not everybody's DNA is unique; as noted above – identical twins, by definition, share the same genetic pattern. And identical twins (also known as monozygotic twins) are fairly common; identical twins happen in about 1 of every 250 births.[1] The incidence of identical twin pregnancies is very similar for all races and age groups. Adopting DNA as a sole identification system would instantly create millions of potential false matches.

Over the past decade, DNA identification has also worked its way into thousands of court cases. The test is thought to be ideal for crimes where no fingerprints are found, and needs only tiny amounts of genetic information for success. Even so, further research and scientific verification is needed to ensure that DNA identification is as accurate as commonly perceived by the average person. Some have suggested that a PIN or password could be used to differentiate between two identical twins; the belief among security experts is that this solution is not appropriate, as it relies too heavily upon the agreement and participation of the individuals involved. Two identical twins in collusion could easily defeat such a system. However, other biometrics could be used to successfully differentiate identical twins, or those that because of coincidence or family genetic makeup have similar DNA (iris patterns for example are different between identical twins and in fact between the two eyes of a given individual[2]).

1. Ventura, Stephanie *et al.* (1999), "Births: Final data for 1999", National Vital Statistics Reports, Vol. 49, No. 1, Centers for Disease Control and Prevention, www.cdc.gov/nchs/data/nvsr/nvsr49/nvsr49_01.pdf, accessed 20 April 2004.

2. Daugman, J and C. Downing (2001) "Epigenetic Randomness, Complexity, and Singularity of Human Iris Patterns", Proceedings of the Royal Society, B, 268, Biological Sciences, pp. 1737 – 1740.

**Existing applications**

Many jurisdictions have forensic identification databases containing DNA samples. Some jurisdictions also have mandatory procedures to deposit the DNA of convicted criminals into their DNA database for matching against DNA material recovered from unsolved crimes. Supporters of these systems note that DNA identification is vital in the solution of some cases.[3]

An extremely large DNA identification databank has been constructed by the US Department of Defense (DoD). The purpose of the Department of Defense DNA Registry is to identify the remains of lost soldiers. As of 2001, the Registry's Specimen Repository had an estimated 3.5 million DNA specimens.

According to a written statement about the repository that appeared on the DoD's Web site:

> The blood is placed on special cards with the service member's Social Security number, date of birth, and branch of service designated on the front side of the card. On the reverse side of the bloodstain card are a fingerprint, a bar code, and signature attesting to the validity of the sample. Ultimately, the bloodstain card is stored in a vacuum-sealed barrier bag and frozen at -20 degrees Celsius, in the Specimen Repository. The oral swab (buccal scraping) is fixed in isopropanol and stored at room temperature. Great care is taken to prevent the possibility of error from sample switching or mislabeling.[4]

Many other DNA storage systems exist, but are not presently being used for identification purposes. These include research databases, blood banks and tissue storage facilities. In spite of the fact that these systems are not ***primarily*** identification systems, care should be taken in the design, architecture and policy development of these systems since the potential exists for new technology to allow these DNA samples to be used to profile and identify individuals.

3. *The Toronto Star* (2003), "DNA links sex attacks", 20 February.

4. US DOD - Armed Forces DNA Identification Laboratory.

## ANNEX IV – BIOMETRIC ENCRYPTION

### Biometric encryption[1]

As indicated earlier in this paper, some consider ***any*** use of template-based biometrics to be potentially privacy invasive.[2] A potential (although not commercially available) solution to the creation of a unique identifier lies in a technology known as 'Biometric Encryption'. In biometric encryption the biometric is used as a key to encrypt and decrypt, but no copy of the biometric sample or template is retained.

Dr. Tomko coined the term 'biometric encryption', in conjunction with a number of US patents that were issued to Dr. Tomko and his various co-inventors between 1994 and 2000.[3] To quote from a presentation supplied to the author directly by Dr. Tomko:

> "The prevailing biometric model, based on retention of the biometric template, is not the only option available. Biometric technology can also be designed as a liberating technology, with the potential to actually enhance privacy, and also, in the process, advance the security associated with public safety. The key is to make the biometric, such as your finger print, the actual encryption key – your own private key, which is never stored anywhere, other than on your finger – that's where it belongs, from a privacy perspective. I call this biometric encryption.
>
> In biometric encryption, you can use the biometric to encrypt a PIN, a password, or an alphanumeric string, for numerous applications – to gain access to computers, bank machines, to enter buildings, etc. The PINs can be 100s of digits in length; the length doesn't matter because you don't need to remember it. And most importantly, all one has to store in a database is the biometrically encrypted PIN or password, not your biometric template."

To understand how biometric encryption works, we first need to look at the functioning of a traditional biometric system. In a traditional biometric system, a template or set of features, or an image is extracted from a biometric sample and stored somewhere in a database. This storage could be in a centralised database or it could be a distributed storage medium such as a smart card. During identification and verification, a comparison is performed between the live person and the stored biometric template.

With biometric encryption we do not store any form of biometric whatsoever, no biometric sample is stored; no biometric template is stored. Instead the biometric sample or template is used as a symmetric encryption and decryption key to cryptographically transform some other piece of information.

When a user enrols, his biometric is used to encrypt a piece of information (it could be any piece of information, an account number, a text string or a credential of some kind). If we call this piece of information 'P', then plaintext 'P' will be transformed into ciphertext 'C' using the biometric 'B'. This

---

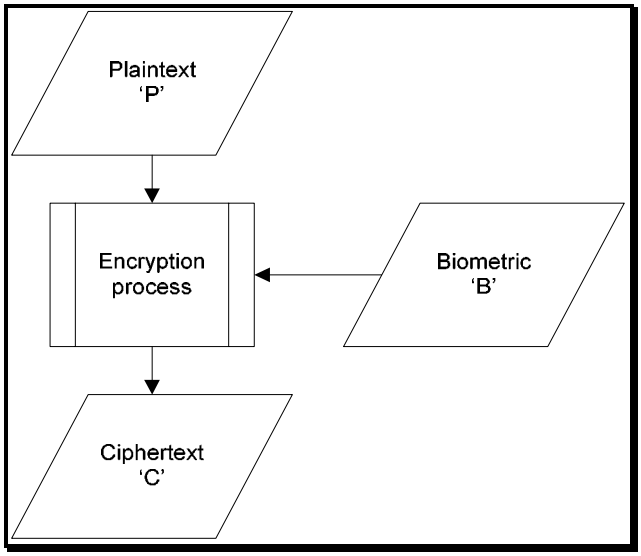
1. There is a pending trademark application on behalf of Bioscrypt Inc. for the term *Biometric Encryption*. (http://strategis.ic.gc.ca/SSG/0806/trdp080643600e.html, accessed 20 April 2004).

2. See Tomko, 2002.

3. The US Patents' numbers directly relevant to biometric encryption are: 5,541,994; 5,680,460; 5,712,912; 5,737,420; 5,740,276; 5,832,091.

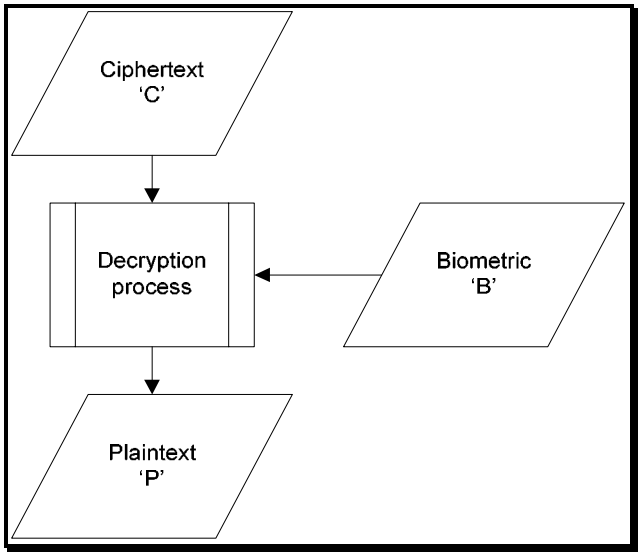
ciphertext is now stored in the biometric encryption system (see Figure 1b). Note, after the encryption process the biometric 'B' is deleted and is ***not stored*** anywhere.

Figure 1. **Biometric encryption enrolment**




When a user identifies or verifies, his biometric is used to decrypt the ciphertext that was stored during enrolment. Ciphertext 'C' will be transformed into plaintext 'P' using the biometric 'B' (see Figure 2b).

Figure 2. **Biometric encryption verification**




The correct user is the ***only person*** who possesses the correct key (his or her biometric) and will be the ***only person*** who can correctly complete the decryption process.

It is challenging to implement this encryption and decryption step, given that each biometric sample or template is distinct for each extraction. We need, what some have referred to as, 'fuzzy encryption' and

'fuzzy decryption'. Interestingly, a solution may be found in technology used to fight spam. 'Nilsimsa Signatures'[4] are fuzzy signatures used to recognise message content as spam, they are able to disregard small changes in text that are statistically insignificant (since spammers will tend to attempt to disguise there messages once they recognised by making changes to the message content). In the same way Nilsimsa signatures may allow us to recognise a biometric which is slightly different each time the user interacts with a system.

Ultimately, biometric encryption does present us with both a key management benefit and a key management problem. While a user can never lose or forget his key (since it literally lives on his body) neither can he effectively 'revoke' a key should it become compromised. This very practical challenge remains to be addressed in the design of biometric encryption.

While biometric encryption would seem to offer a solution to the majority of privacy concerns related to biometric-based technology, it is not, unfortunately, readily available to deploy today.

A number of companies hold patents and have prototype technology and systems based on these patents, but the author is not aware of any ongoing research to bring these systems to market.

4. See *Vipul's Razor*, www.brics.dk/~engberg/usr_local_doc/razor-agents-shr-2.36/README, accessed 20 April 2004.