



Author: Monica Cardenas

Biometry and the Law

Table of content

Introduction

1. Biometric Systems

1.1 Types of Biometry

1.2 Description of most important commercialized biometric techniques

- Fingerprints
- Hand Form
- Face Form
- Voice
- Iris
- Retina
- Thermography
- Various

2. Legal environment and impacts on the protection of personal information and privacy

2.1 Collection : Necessity and consent

2.2 Finality and uses

2.3 Confidential Nature: Conservation and autodestruction

2.4 Access by organisation's personnel

2.5 Communication

2.6 Access and Correction Rights

2.7 Creation of biometric characteristics bank

3. Conclusion

INTRODUCTION

Since the tragic events of September 11th, 2001, safety has become a priority like never before. This event combined with increasing incidents of cyber attacks perpetrated during the last year has pushed governments and companies to seek new computer security technologies. Biometrics remains a field in computer security in which significant growth is expected.

By using biometric technology, the body itself becomes a password. Computerized scanners confirm the identity of a person by collecting information on a distinctive biometric attribute, converting it into extremely complex algorithms, then by comparing the data with a digital file in order to determine if there is a match.

A large number of biometric systems are under development, centered on measuring the distinctive characteristics of various parts of the body. These distinctive attributes can be either physical or behavioral.

All biometric technologies have their advantages and disadvantages. These technologies are measured and compared using many characteristics such as individuality, universality, permanence, possibility of gathering of information, acceptability and possibility of defeat.

If we continue to follow the current trend, biometric technology will soon take a significant place in every day life. But its generalized use raises questions with respect to privacy. What would you say if your fingerprints circulated in cyberspace?

The prospect for increased safety is reassuring. However, the great debate surrounding biometrics and its effects on fundamental freedoms must, and will, continue. This scope of this document is to describe the repercussions and familiarise the reader with laws that relate to biometrics.

1. BIOMETRIC SYSTEMS

"Perhaps the most beautiful and characteristic of all superficial marks are the small furrows with the intervening ridges and to their pores that are disposed in a singularly complex yet even order on the under surfaces of the hands and the feet."

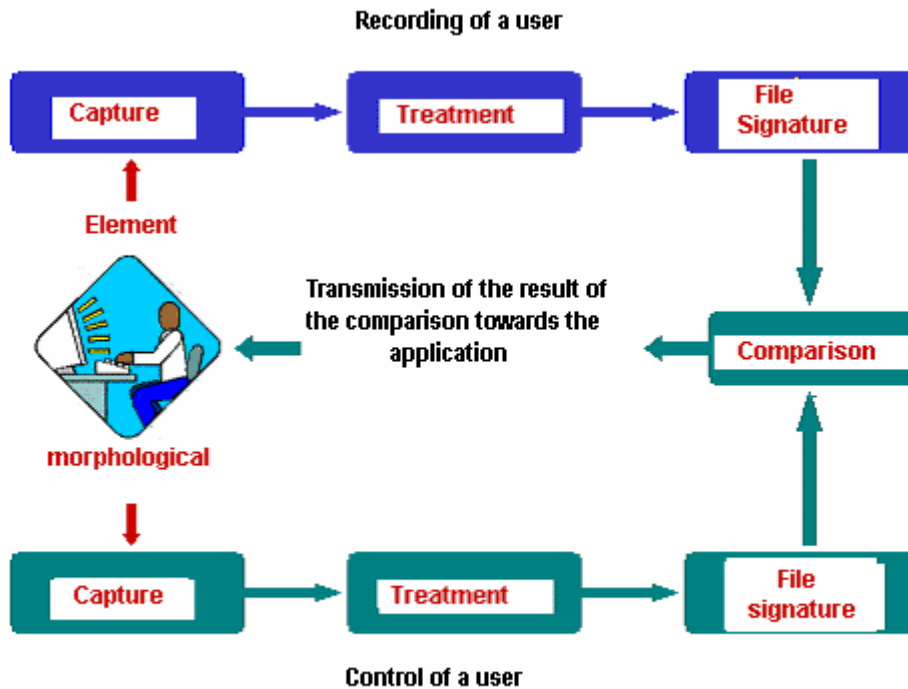
- Personal Identification And Description, Nature, Sir Francis Galton, June 28 1888.

The use of fingerprints, now considered banal, marked the first time it became possible to develop a system for identification of criminals to the police services of the world.

Of all biometric technologies available on the market, those involving the digital measuring of fingerprints remains the most current (about half the market).

Although there are many biometric techniques, they all work using a similar scheme. First of all, any biometric system requires an initial input of data. To do so, a reading from physiological or behavioral characteristics of the person is made by a biometric capture terminal. The parameters resulting from this reading are processed to generate a unique "signature". Each signature is then recorded in a central database or sometimes in a portable device. This whole process is known as enrolment:

- 1 – Biometric reading terminal
- 2 – Identity verification
- 3 – Comparison of the reading with recorded "signatures"
- 4 – Data deposit
- 5 – "Signature" file
- 6 – Physical or behavioural characteristic reading
- 7 – Match? Yes/No
- 8 – Acceptance/Refusal



1.1 Types of Biometry

Biometric systems are generally classified by the industry in two major categories: morphological or physiological biometry and behavioural biometry.

Morphological biometry is based on the identification of particular physical traits that are unique and permanent to every person. This category includes fingerprints, hand form, face form, iris and retina scans.

Behavioural biometry is rather based on the analysis of specific behaviours of a person like writing a signature, speaking or typing on the keyboard. We will add to those two categories a third one, consisting of the study of biological traces, like DNA, blood and odour analysis.

New techniques are currently under development and it would not be surprising to see them added to those already commercialized or mentioned above.

1.2 Description of Biometric techniques

- Fingerprints

One of the best-known techniques, it is also the oldest. It is because of the works of Alphonse Bertillon, in the 1880s, that we first were able to identify recidivists without having to use marking or mutilation.

The idea of using this technique as an identification instrument in itself came with the study of British researcher Sir Francis Galton, who demonstrated the permanence of the drawing, its inalterability and its individuality.

Fingerprint Minutiae:

Fingerprint minutiae, according to Galton, is the particular arrangement of the papillary lines forming characteristic points and is the origin of the individuality of the digital drawings. Line stops, bifurcations, lakes, isles, points, the combination of minutiae is practically infinite. In the legal practice of developed countries, between 8 and 17 points (but most often 12) without discordance are needed to consider the identification established. The technology mostly used for image capture was optical (lighting + prism + CCD camera), up until now. New generation scanners (with silicon chip) are smaller and cheaper, which means this technology can be adapted to fit nearly all conceivable applications, even cell phones.

- Hand Form

The hand silhouette is a characteristic of every individual. The hand form is acquired through a specialized scanner, generally infrared. Parameters like digits lengths, their thickness and relational positions are extracted from the image and compared to the database. This biometry is however subject to modifications of the hand form related to aging.

- access control
- easy to use, it is still too large to use on a desk, car or phone

- Face Form

The distance between the eyes, nasal spacing or mouth width can allow to identify an individual. This method must be accountable for certain changes of physiognomy (glasses, beard, esthetic surgery) and environment (lighting conditions). It is impossible to differentiate two twins.

The face is a relatively unsafe biometry. Indeed, the acquired signal is subject to higher variations than most other characteristics. Those variations can be caused by, among others, make-up, pilosity, presence or absence of glasses, aging and emotional expression. The face authentication method is sensible to lighting variations and face positioning changes while capturing the image. Also, it is recommended to use the same type of camera in many applications. Many commercial products have already appeared on the market.

- Voice

A person's voice is characterized by many parameters. Each person has his own voice that can be analyzed with a microphone recording.

The sounds are characterized by a frequency, a tone and a volume. The computer processing takes account of distortions related to the equipment in use and can even analyze low quality samples, like telephone or radio transmissions.

Fatigue, stress, or a cold can provoke variations of the voice. Fraud is possible if the voice of someone is recorded without his knowledge. To prevent that, one technique is to force someone to read a random text that changes every time.

- Iris

The person who wants to be identified simply looks at the camera that instantly catches an image of his iris. The iris is a very dense motif that is not dictated by genes. Each eye is unique. In every iris photography, there is more than 200 independent variables, which makes the probability of mismatching 2 individuals very unlikely. This method was invented by ophthalmologists in the 1980s, who discovered that the colour of the iris can change, but rarely its motif. This method of identification will certainly continue to evolve with the time, probably as much as the fingerprints, at least as much as the evolution of cameras.

To capture an image of this colored membrane, there is no need to shine light on the retina. However, the lighting of the iris poses a problem with reflections, we often use calibrated artificial lighting (DEL diodes) while minimizing the ambient light. The lighting is easy to tolerate since it can be infrared, nearly invisible to the person. The system can be fooled by using a picture or a contact lens reproducing the iris of the subject we want to impersonate. But the resolution required by the scanner is really high (distance between iris and camera is very small, rapid evolution of CCD/CMOS captors technology). Also, it is possible to notice, through filtering, that the image of the iris shown is made of dots following a regular pattern and not various motifs.

- Retina

The retina is the sensorial layer of the eye that allows vision. This zone is traveled by blood vessels who emerge at the level of the optical papilla, where we distinguish the central retinal artery and vein which divide themselves into smaller diameter arteries and veins to supply blood to the cells. The great variety of blood vessels configurations offers the same diversity as the fingerprints. The image of the blood vessels can be altered by age or sickness, but the relational position of the vessels according to each other is unchanged throughout the lifetime of a person. A camera is used to record the cartography of the vessels, to do so, it is necessary to shine light through the pupil.

- considered like the most reliable biometric method, suffers from psychological reserve from the user, people have difficulty accepting the idea of a light ray going through their eye
- this vascular map is unique even if the subjects are twins and changes very little throughout a lifetime
- studies with ATMs already exist in some countries
- “high security” access control, but the product will remain higher priced than others using a different technology because there is no mass production

- Thermography

A thermal camera is used to take an infrared picture of the face. This allows to highlight a unique distribution of the heat across the face of every individual, in other words to map the invisible blood vessels network. The main advantage is to be able to differentiate real twins. Very costly, this system is still experimental.

- Various

The hear can sometimes be used by the police to identify a suspect from picture taken on the site of the crime. The teeth, the odor, the heart's beat, the blood irrigation and many other techniques of biometric identification are currently under study at an experimental stage. Why not DNA analysis? However, it is still too early to predict any industrial usage.

The methods and techniques listed above are all directed by common principles:

Sensor: A system of sensor (microphone, scanner, camera) must transmit useful data from the individual to be identified to a central system.

Analysis Software: A software or chip must compare the data transmitted to the data stocked and authorize or deny access.

Central Database: A central computer must possess a copy of the data allowing for the identification: fingerprints, vocal signature or other.

2. LEGAL ENVIRONMENT

The use of biometric identification techniques raises, justly, great concern. From a legal standpoint, some of the uses could violate various rights and guarantees protected by our Charters, like the freedom of religion, the freedom of conscience and the right of respect to their privacy. Some critics associate such biometric data to a high tech marking. In order to reassure those who fear to see such data would be used for wrong purposes, within the set of Canadian legal requirements, Quebec is in the forefront of industrialized countries in the matter personal data protection. In Quebec, personal data protection is regulated by two laws of enforcement, the <<Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels>> (L.R.Q., c. A-2.1) (Law on access to personal data) and the <<Loi sur la protection des renseignements personnels dans le secteur privé>> (L.R.Q., c. P-39.1) (Law concerning the private sector).

The protection against abusive search by police authorities is another source of preoccupation. However, the legislator as expressly authorized, but under a specific set of rules and in order to counter crime, the use of biometric identification techniques like taking blood samples or body substances (hair, fingerprints, etc.) Even if the right to privacy or the inviolability of the person must be overshadowed by public interest, the legislator has drawn borders to guarantee that the techniques and results must be used for specifically approved ends.

For example, the city of Toronto plans to put in place an encoded fingerprint system in its new "Client Identification and Benefits System" in order to fight social security fraud. The risks towards private life have been examined carefully by the Office of the Commissioner to Information and Privacy Protection ***find exact title***. It is important to note that encoded fingerprint readers are targeted to a very specific usage, to fight a particular fraud called benefits accumulation, which consists in obtaining many checks of social security benefits while using fake identities. This type of fraud is frequently observed in benefits programs, does not exist only in Canada.

The legislator has considered reasonable, under certain circumstances dictated by the jurisprudence, to restrain the right to privacy of an individual, in the face of legal or criminal procedures. The Canadian Charter of Human Rights and Freedoms stipulates five necessary conditions:

- 1- Beforehand authorization of a neutral and impartial person capable of acting with legal authority.
- 2- Existence of reasonable doubts that a crime has been committed
- 3- Proofs of this crime should be located at the searching place
- 4- Execution of search warrant must not be abusive

- 5- The ***justiciable*** must be able to control a posteriori the constitutional validity of the process. In the event that the case is abandoned, dropped or late, there will be destruction of all proof elements, records, test results or other.

In the work relations domain, biometric techniques have also been used as verification tools and well-being insurance in work environments where mistakes resulting from human weaknesses caused by drugs, sickness or other physical condition can't be tolerated. The Supreme Court of Canada stipulated that the requirements must comply with a <<*condition d'emploi adoptée honnêtement pour de bonnes raisons économiques ou d'affaires, également applicables à tous ceux qu'elle vise*>>.

In a computer environment, special measures are taken to insure the functional equivalence of a document and its judicial value. Also, when the person's identity linked to a document is guarded by a biometric method, this new law finds its application in conjunction with the <<*Loi sur l'accès*>> (Law on access to personal data) and the <<*Loi dans le secteur privé*>> (Law concerning the private sector) depending if the usage of the law applies to the public or the private sector.

More recently, the legislator has introduced specific dispositions concerning biometry in articles 44 and 45 in section II of chapter III of the <<*Loi concernant le cadre juridique des technologies de l'information*>> (L.Q. 2001, c.32) (Law on information technologies). Those articles are put as follows:

44. Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance.

Tout autre renseignement concernant cette personne et qui pourrait être découvert à partir des caractéristiques ou mesures saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit. Un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande.

Ces caractéristiques ou mesures ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

45. La création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service.

La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne.

La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée.

So, the various laws in effect dictate the rules applying to the collection, use, conservation and communication of the data collected upon which the public administration and private enterprise must based themselves.

2.1 Collection: Necessity and Consent

The collection of personal data is regulated under the rule of necessity (article 64 of the <<Loi sur l'accès>>; articles 4 and 5 of the <<Loi dans le secteur privé>>). The notion of necessity has always been interpreted, by the Commission, in its strict and rigorous meaning, as a synonym of unavoidable. This necessity is better appreciated in its context.

Those imperative dispositions force the organization willing to proceed to the collection of biometric data to demonstrate, not only as a simple utility or commodity, but the fact that we it cannot rigorously do without.

The consent of the person to provide personal data does not allow to overshadow this rule.

The <<Loi sur les technologies de l'information>> (Law on information technologies) adds a new obligation whenever occurs the collection of biometric data: the expressed consent of the concerned person.

It is beforehand excluded that the collection of data might be done otherwise than with the concerned person. So, those biometric measurements can't be collected without the knowledge of this person, whether it is during the hiring or verification of the identity.

Also, it is required to receive the expressed consent during the collection of the biometric measurement. The Commission, in the matter of consent, as determined the qualities of a valid consent. It has to be free, enlightened and given for specific uses.

- The choice of someone to be identified by a biometric method has to be respected. The refusal to use such a method must overcome even with the demonstration of necessity.
- An enlightened consent has to allow an individual to understand the impacts of the use of biometry and be to know how the collected data will be protected, used, shared and when it will be destroyed.
- A given consent towards specific ends should allow the person to know precisely what data will be collected and used.

Also, article 44 specifies that a minimal quantity of characteristics can be collected when justified.

2.2 Finality and Uses

To justify the necessity of the collection of personal biometric data, one must first determine the finality pursued by the constitution of such a file and the uses that will be made of it. Those uses must be declared to the concerned person at the time of the collect (article 65 of the <<Loi sur l'accès>> and article 8 of the <<Loi dans le secteur privé>>).

In the legal environment covered by the <<Loi sur les technologies de l'information>>, the biometric data will serve essentially to identify the individual in order to associate a document. The necessity to identify the person in the prospect of the finality pursued must be intrinsically unavoidable

So, the biometric measurements collected from an individual can only be used to identify that individual and any other usage or information revealed by those measurements cannot be used to any other end.

2.3 Confidential Nature: Conservation and autodestruction

Biometric measurements, like most personal data, are confidential and must be protected by specific requirements able to insure their confidential nature (article 53 of the <<Loi sur l'accès>> and article 10 of the <<Loi dans le secteur privé>>). The quality of the recorded data must be protected in order to use exact and up to date information (article 72 of the <<Loi sur l'accès>> and article 11 of the <<Loi dans le secteur privé>>). The integrity of the recorded information is crucial when it is biometric measurements since its function of identification of an individual cannot be approximate without risking discrimination

The biometric measurements are linked to a more urgent destruction requirement. It is clearly stated in article 44 that those measurements must be destroyed when the object of the identification is accomplished or when the reason behind it does not exist anymore.

2.4 Access by the organization's personnel

Access by the personnel of the organization who collected the biometric data is usually restricted to those who have quality to receive and must access this personal information in the exercise of their duty (article 62 of the <<Loi sur l'accès>> and article 20 of the <<Loi dans le secteur privé>>).

In regards to biometric data, access privileges should be restrained as much as possible since the enrolment and identification process is an integral part of the biometric systems and the biometric data should not be manipulated directly.

2.5 Communication

The communication of personal information, including biometric data, requires the consent of the concerned individual or a legal disposition that authorizes this communication (article 62 of the <<Loi sur l'accès>> and article 20 of the <<Loi dans le secteur privé>>).

2.6 Access and Correction Rights

The access right and the right to correction of personal information held by the public administration (articles 83 and 89 of the <<Loi sur l'accès>>) or a private company (articles 27 and 28 of the <<Loi dans le secteur privé>> and article 40 of the *Code civil*) remain applicable to biometric data.

2.7 Creation of biometric characteristics bank

The article 45 of the <<Loi sur les technologies de l'information>> initiate a new obligation for organizations which desire to use biometry and create a bank of biometric measurements. Prior to the creation of such a bank, those organizations must inform the Commission of such a project. Also, currently existing banks, in operation or not, will also have to be signaled to the Commission.

The Commission has power concerning those personal data banks. It is allowed determine the creation, use, consultation, communication and conservation, as

well as prohibit or suspend the deployment of a bank. It can also order its destruction if it becomes a threat to personal privacy.

3. CONCLUSION

In the biometry context, the threat to individual rights and privacy does not come from the positive identification of the person, but from the capacity of third-party entities to access the personal data in an identifiable form and link it with other information, which leads to a secondary usage of the data without the consent of the targeted person. This means that the individual does not have control anymore over information concerning himself. The respect of privacy is defined by the capacity to dictate the use and diffusion of the personal data concerning the individual, it is linked to the freedom of choice. Without the possibility of using a certain control over the use of one's personal data, the respect of privacy becomes an empty notion.

The efficacy and usefulness of the biometric identification techniques, depending on the objective, is such that we cannot hope to abolish or eliminate not only their usage, but also their evolution and expansion. However, we will have to insure that the use of such techniques will be made in just balance between society's needs and individual rights and freedoms protection.