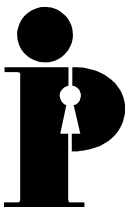
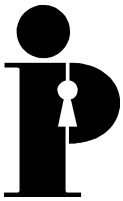
Information
and Privacy
Commissioner/
Ontario

Privacy and Biometrics



Ann Cavoukian, Ph.D.
Commissioner
September 1999



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1V8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Cette publication est également disponible en français.

This publication is also available on the IPC website. Upon request, this publication will be made available on audio tape to accommodate individuals with special needs.

Abstract

It is possible for biometric technology to be used in a manner that does not compromise informational privacy, in both public and private sector applications. However, targeted legislative, procedural and technical safeguards are necessary to ensure privacy is protected.

Biometric systems can be designed to put the power of the biometric into the hands of the individual, as opposed to the government, the police, or big business. Applications can be configured to give the data subject the ability to control access to his or her own biometric data, to safeguard the integrity of his or her personal information, and to protect his or her identity against theft or misappropriation.

Recognizing the potential of biometrics to enhance security and privacy prompted the Office of the Information and Privacy Commissioner of Ontario, Canada, to work with public and private sector organizations to effectively identify and address privacy concerns prior to the implementation of biometric technology.

Table of Contents

Introduction

Over the last year, the Office of the Information and Privacy Commissioner/ Ontario (the IPC) has been examining the privacy implications of biometric technology. The IPC believes that if left unregulated, this technology could be used in ways that could compromise informational privacy.

However, the IPC also believes that if properly designed and regulated, this technology could actually be a means to enhance privacy.

The IPC is studying the use of biometrics in three areas — government, law enforcement, and consumer applications — with the objective of reassessing the specific privacy concerns associated with this technology, and then defining the privacy protective standards necessary to effectively address those concerns.

Privacy Friend or Foe?

Biometrics have traditionally been shunned by privacy advocates, for a number of reasons. On the face of it, however, the primary reason advanced arises from the association of biometrics, primarily fingerprints, with criminality. Fingerprints have historically been used by law enforcement agencies to track down those suspected of committing criminal acts. For this reason, fingerprints have raised concerns over loss of dignity and privacy. Furthermore, the central retention of fingerprints and multiple access by different arms of government tends to evoke images of "Big Brother" surveillance.

When considering the privacy concerns associated with biometrics, an important distinction must be made between identification and authentication. A computer system can be designed to identify a person based on a biometric characteristic. To do this, it compares a biometric presented by a person against all biometric samples stored in its database. If the presented biometric matches a sample on file, the system has identified the individual. This is called a "one-to-many" match, and is used by the police to identify criminals, as well as by governments to identify qualified recipients for benefit-entitlement programs and registration systems such as voting, driver's licenses and other applications.

Authentication involves a "one-to-one" search whereby a live biometric presented by a person is compared to a stored sample (on a smart card, for example) previously given by that individual, and the match confirmed. The eligibility of the person for the service or benefit has been previously established. The matching of the biometric is all that is necessary to authenticate the individual as an eligible user. There is no searching or matching to a central database.

Authentication does not require identification each and every time an eligible individual uses a service. In addition, unlike biometric identification, authentication does not necessarily require the biometric be stored in a central database. A template could be stored on a card, in the possession of the individual, thereby putting the control over access in the hands of the data subject.[1]

Privacy fears are justified in the context of identifiable fingerprints of the kind commonly used by the police, where there is centralized retention. A fingerprint, and the broader family of biometrics, including voice prints and body parts such as the retina, iris, and hand, offer irrefutable evidence of one's identity since they are unique biological characteristics that distinguish one person from another, and that only can be linked to one individual.

When identifiable, fingerprints, or indeed any biometric, can act as a powerful unique identifier that can bring together disparate pieces of personal information about an individual. If used in this manner, a fingerprint enables individuals to be pinpointed and tracked. It also creates the potential for personal information from different sources to be linked together to form a detailed personal profile about that individual, unbeknownst to him or her. This represents a clear invasion of privacy; one to which most people would object.

When biometrics are examined beyond the surface image of the "common criminal" model, a different image emerges. By going beyond this common linkage, what is really at the heart of the traditional opposition to biometrics (from a privacy perspective) can be examined. In order to see this more clearly, the question must be asked: what would make a biometric become a protector of privacy?

The threat to privacy arises not from the positive identification that biometrics provide best, but the ability of third parties to access this data in identifiable form and link it to other information, resulting in secondary uses of the information, without the consent of the data subject. This erodes the personal control of an individual over the uses of his or her information. Informational privacy is defined as the ability to maintain control over the use and dissemination of one's personal information. It revolves around freedom of choice and personal control — informational self-determination.

Threats to privacy can arise from the use of identifiable (raw image) biometrics that can function as a unique identifier (such as the Social Insurance Number in Canada or a driver's licence). As with all unique identifiers, it is the secondary uses of personal information that cause the greatest concern, and the subsequent linkages that may be achieved through the use of the unique identifier.

However, the IPC recognizes that biometric technology does not have to be used in such a manner. With the application of encryption to biometrics, it is hoped that the technology can evolve to the point where systems can be designed to put the power of the biometric into the hands of the individual, as opposed to the government or big business. Also, certain types of encryption may be able to address the security vulnerabilities inherent in biometric technology.[2] Applications can be configured to give the data subject the ability to control access to his or her own biometric data, to safeguard the integrity of his or her personal information, including the biometric, and to protect his or her identity against theft or misappropriation.

Recognizing this potential of biometrics to enhance security and privacy prompted the IPC to examine how the technology could be used, in various applications, in a manner that does not infringe on informational privacy. In Canada, biometric applications are still limited primarily to the area of law enforcement. This gave the IPC the opportunity to work with public and private sector organizations to effectively identify and address the privacy concerns prior to the implementation of the technology.

Biometrics and Government Programs

As is the case in numerous jurisdictions around the world, various levels of government in Ontario are looking to implement measures designed to effectively fight fraud in their benefit-entitlement programs. One form of fraud of particular concern is "double-dipping," where an individual unlawfully obtains benefits under multiple identities. This form of fraud is not unique to Ontario, but quite prevalent in certain types of government benefit programs. As one source noted:

Fraud is a significant issue in public-sector programs. A persistent problem of state welfare entitlement programs is fraud perpetrated by double dippers — individuals who illegally register more than once for benefits by using an alias or other false information. Many experts believe that fraud in programs like welfare can be as high as 10%, which translates to over $40 billion a year in potential savings if the fraud was prevented.[3]

When it became clear that the City of Toronto was considering the introduction of a biometric measure in its efforts to control welfare fraud, the IPC (as the provincial oversight agency responsible for the protection of privacy in Ontario) worked with the City, as well as the Ministry of Community and Social Services, the provincial organization in charge of welfare across the province, to develop a legislative framework that would define the necessary privacy safeguards.

As a starting point, the IPC developed a list of procedural and technical safeguards that it believed should be present when biometric technology is used. Further, the IPC recommended that these safeguards be enshrined in legislation, in order to give them the force of law.

The IPC insisted that whatever biometric was used had to be encrypted; this in itself was an unprecedented requirement, not previously in existence in other statutes relating to the use of biometrics. The IPC's proposal to the government was that the following procedural and technical privacy safeguards should be in place prior to the implementation of any biometric technology:

- the biometric (in the case of the City of Toronto, it was a finger scan) should be encrypted;
- the use of the encrypted finger scan should be restricted to authentication of eligibility, thereby ensuring that it is not used as an instrument of social control or surveillance;

- the identifiable fingerprint cannot be reconstructed from an encrypted finger scan stored in the database; ensuring that a latent fingerprint (i.e., one picked up from a crime scene) cannot be matched to an encrypted finger scan stored in a database;
- the encrypted finger scan itself cannot be used to serve as a unique identifier;
- the encrypted finger scan alone cannot be used to identify an individual (i.e., in the same manner as a fingerprint can be used);
- establish strict controls on who may access the biometric data and for what purposes;
- require the production of a warrant or court order prior to granting access to external agencies such as the police or government organizations;
- any benefits data (i.e., personal information such as history of payments made) are stored separately from personal identifiers such as name or date of birth.

The Ontario government passed the *Social Assistance Reform Act* which, while not identical to the IPC's recommended safeguards, came fairly close. The IPC believes the legislation is unprecedented with respect to the breadth of the privacy safeguards regarding the use of an encrypted biometric. The following protections are enshrined in the legislation:

- any biometric information collected under this Act must be encrypted;
- the encrypted biometric cannot be used as a unique identifier, capable of facilitating linkages to other biometric information or other databases;
- the original biometric must be destroyed after the encryption process;
- the encrypted biometric information only can be stored or transmitted in encrypted form, then destroyed in a prescribed manner; and
- no program information is to be retained with the encrypted biometric information.

Further, the statute includes the following provision:

> 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.

Therefore, the biometric technology selected must not be capable of either reconstructing or recreating an original biometric pattern from the encrypted biometric nor having it matched to a copy or reproduction of a biometric not obtained directly from the individual (i.e., a latent fingerprint taken from a crime scene). As a result, the database containing the encrypted biometrics of welfare recipients would be of little interest to the police. However, should they or any other third party want to access the biometric information, they only could do so through the production of a court order or a warrant. Otherwise, they would not be permitted access to the data.

Also, the collection of the biometric information must be conducted in an open manner. As stated in the statute: "Biometric information to be collected from the individual to whom it relates shall be collected openly and directly from the individual."

The City of Toronto biometric initiative has not been implemented as of the date of this paper. However, the IPC believes the legislative framework introduced will provide effective privacy protection for government benefits-entitlement application of biometrics in Ontario. The IPC also believes that the *Social Assistance Reform Act* could provide a useful model for other jurisdictions beginning to consider the use of biometric technology to fight fraud in government programs and services. The relevant sections of this legislation, containing the complete set of safeguards relating to the use of encrypted biometrics, may be found in Appendix A.

Biometrics and Policing

The IPC contributed a chapter on biometrics and policing to the proceedings for the Sommerakademie 1999 in Kiel, Germany.[4] In that document, the IPC recognized the potential harm from the misuse of biometrics as significant, but further argued its position that the key point for discussion about biometrics was not that the technology should not be used because it posed a threat to privacy, but rather, when used, it must be used responsibly.

Biometrics and policing are not strangers to each other. Fingerprints have been used for the identification of suspects and victims for more than 100 years. Although crude in form, facial recognition through photographs and sketches, à la the "most wanted" posters, have been used for an even longer time.

The law enforcement community is the largest biometric user group, making up 50% of biometric spending in 1998.[5] Police forces throughout the world use Automated Fingerprint Identification Systems (AFIS) to process criminal suspects and match finger images. Various other forms of biometrics are used to secure prisons, police detention areas, enforce home confinement orders, and regulate the movement of probationers and parolees.

Law enforcement is increasingly coming to rely on the use of DNA-based technologies as an aid in solving crimes. Although not yet at the point of other biometric technologies in terms of speed, DNA matching cannot be ignored. DNA is being used to process criminal suspects to separate the guilty from the innocent. It is also being used to identify victims and to match convicted offenders to outstanding crimes. To aid these processes, the establishment of DNA data banks is either under way or under consideration in several jurisdictions, including Canada.

The benefits of biometrics to law enforcement efforts are well documented. However, in order to realize those benefits, biometric data must be identifiable. This gives rise to a number of significant informational privacy concerns. The use of DNA raises the potential of additional privacy issues if used for purposes beyond identification to obtain, for example, information about health-related predispositions or ethnic background.

However, in the context of law enforcement, it is important to note that privacy is not an absolute right. Data protection legislation in Canada, as well as in other jurisdictions, balances individuals' privacy rights with larger societal concerns. The IPC maintains that whenever a balance between individual and societal needs must be struck, the development of legislation is perhaps the best way to achieve this balance. Accordingly, it is the IPC's position that the use of biometrics should be regulated by legislation.

In addition, the IPC believes the policing community has two critical roles to perform as the use of biometrics increases. First, it can control its own use of biometric information. The rights of the individual regarding identification have been firmly established in many areas. Just because those rights have not yet been as firmly defined in the specific area of biometrics does not mean that police should make use of the technology in ways inconsistent with how they use any other identification methods.

Second, those inexperienced with biometric technology, be they businesses, employers, social-benefits administrators or others, need guidance in the proper use of this powerful technology. As experienced players, the police may have a role in influencing the larger community toward a positive direction for the use of biometrics. This will depend entirely on the role the police choose to adopt in the future.

Biometrics and Consumer Applications

The third area where the IPC has examined the use of biometrics is in business applications directed at consumers. Various research firms and industry experts anticipate the growth of the biometric industry to be significant in the near future:

- One industry study said that biometrics will expand to a $1 billion industry by the year 2000.[6]
- In 1997, Bill Gates, Microsoft Corporation, predicted that biometric technologies will be one of "the most important IT innovations of the next several years."[7]
- Some experts even predict that the rush to install biometric security systems will replace the Year 2000 computer crisis as the most pressing high-tech project after the millennium.[8]

Regardless of the prediction, it is clear that the commercial use of biometrics is expanding worldwide. As examples, facial and iris recognition are being incorporated into Automated Teller Machines; financial institutions are using fingerscanning to identify clients; and finger geometry is used to control access to major theme parks.

There are indications that public understanding and acceptance of biometrics is increasing. For example, one American survey indicated that 87% of respondents thought fingerprinting was a legitimate identification requirement. The survey found that 91% believed that it was justified to use finger imaging to control entry to high security areas, 77% to verify the identity of persons cashing personal cheques for large amounts; and 76% to identify persons using credit cards for major purchases. More than four out of five (83%) respondents rejected the view that using finger imaging to verify people's identity was treating them like presumed criminals.[9]

While consumer biometric applications are still rare in Canada, the IPC anticipates Canada will not be exempt from the significant growth in the technology's use.

Accordingly, to help ensure the introduction of biometrics into the commercial environment does not unduly compromise privacy, the IPC has published *Consumer Biometric Applications: A Discussion Paper*, which is designed to give consumers an overview of the technology, explain how and why it is used, the potential benefits associated with the technology for both business and consumers, as well as outline a number of privacy issues and questions they should consider prior to consenting to the use of their biometric.[10]

In particular, the IPC's position is that in the absence of data protection legislation for the private sector, or specific legislation regulating the use of biometric identifiers, consumers need to represent and advocate their own privacy interests regarding their biometric data. To do so, they need to be aware of both the benefits and dangers associated with biometrics in order to make an informed choice about whether to participate in consumer biometric applications.

The IPC advises consumers that when they enrol in most biometric systems, they may be required to relinquish control over something that is highly personal and virtually immutable. Caution is advisable. However, the IPC also contends that biometrics need not subvert informational privacy. A pro-privacy position should not be construed as an anti-biometric stance.[11]

Biometric data, itself, can serve as an effective security safeguard when it is controlled by its owner (e.g., to restrict access to one's information by acting as one's private encryption key, or as an access control mechanism to secure a physical area or device containing confidential information). If at all possible, consideration should be given to whether the consumer biometric application can be designed so that consumers can have control their own biometric data.

The IPC believes that the informational privacy concerns associated with biometrics can be effectively addressed if the technology is used in accordance with fair information practices. In *Consumer Biometric Applications: A Discussion Paper*, the IPC examines each of these principles in terms of its applicability to privacy protection for biometric data. In addition, the IPC recommends a number of procedural and technical privacy safeguards for consumer biometric applications.

Conclusion

Two things are certain:

1) the use of biometric technology by government, law enforcement and business will grow dramatically in the next decade — industry observers believe the potential applications are infinite. "Any situation that allows an interaction between man and machine is capable of incorporating biometrics;"[12] and

2) the existence of stringent safeguards — legislative, procedural and technical — will become essential to ensure that biometrics do not pose a threat to informational privacy.

Whether biometrics are privacy's friend or foe is entirely dependent upon how the systems are designed and the information managed. The technology can actually be privacy enhancing if designed with that objective in mind.

It would be short-sighted, at best, for the data protection community to reject all biometrics, across the board, as privacy-invasive. Government, law enforcement and business applications are growing worldwide. Accordingly, the data protection community must act now to ensure that public and private sector organizations considering biometric technology recognize that its use needs to "conform to the standards and expectations of a privacy-minded society."[13] The community has a responsibility to critically examine the benefits, as well as the concerns, associated with biometrics, and then to move decisively to ensure that this technology does not knowingly or inadvertently compromise informational privacy.

References

1. George Tomko, "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?," Privacy Laws & Business 9th Privacy Commissioners/Data Protection Authorities Workshop, Spain, September 15, 1998 (as of 7/5/99), www.dss.state.ct.us/digital/tomko.htm.

2. George Tomko, "Privacy Implications of Biometrics — A Solution in Biometric Encryption," Eighth Annual Conference on Computers, Freedom and Privacy, Austin, Texas, 1998.

3. John D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?," *Proceedings of the IEEE*, Vol. 85, No. 9, September 1997, p. 1487.

4. The proceeding's website is at: www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/tb/tb21/kap13.htm, (as of 6/23/99.) The IPC paper appears in *Polizei und Datenschutz*, Dr. Helmut Bäumler, Editor (Luchterhand Verlag: 1999). As of August 23, 1999, the IPC's paper is available on its website at: www.ipc.on.ca.

5. "Big Brother biometrics: The identification you'll never leave home without," CNN fn Digital Jam, August 26, 1998 (as of 12/29/98), japan.cnnfn.com/digitaljam/redherring/9808/26/redherring_biometrics/.

6. "Moving Beyond Passwords: Biometrics to Introduce Retina Scans, Voices, Prints," ABCNews.com, November 18, 1998 (as of 4/21/99), abcnews.go.com/sections/tech/DailyNews/net_security981118.html.

7. Integrated Telecommunications Systems Canada Inc., "For Canadian Companies, Biometric Identification and Access Control Should Go Hand-in-Hand," News Release, September 23, 1998.

8. "Moving Beyond Passwords," ABCNews.com, November 18, 1998.

9. Alan F. Westin for The National Registry Inc., "Public Attitudes Toward the Use of Finger Imaging Technology for Personal Identification in Commercial and Government Programs: Results of a National Public Opinion Survey conducted by Opinion Research Corporation's Caravan," August 1996, pp. 3–4.

10. *Consumer Biometric Applications: A Discussion Paper* is available on the IPC website: www.ipc.on.ca.

11. Testimony of John D. Woodward Jr. to the Hearing of the Subcommittee on Domestic and International Monetary Policy, Committee on Banking and Financial Services, U.S. House of Representatives, One Hundred Fifth Congress on "Biometrics and the Future of Money," Washington, D.C., May 20, 1998 (as of (4/22/99), www.dss.state.ct.us/digital/legal1.htm.

12. Gary Roethenbaugh, *ICSA Biometrics Buyer's Guide*, Chapter 3 — The Need for Biometrics (as of 6/24/99), www.iCSA.net/services/consortia/cbdc/bg/chap3.shtml.

13. Simon G. Davies, "Touching Big Brother: How biometric technology will fuse flesh and machine," Information Technology & People, Vol. 7, No. 4, 1994 (as of 12/29/98), www.interlog.com/~cjazz/biometric.htm.

Appendix A

Social Assistance Reform Act

"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 authorize 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 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 authorized provider.

    4. To enable an applicant, recipient, spouse 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 authorized 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.

(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.

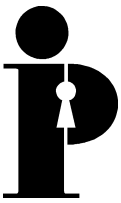
(5) An administrator shall ensure that biometric information can be accessed and used only by those persons who need the information in order to perform their duties under this Act and that it is not used as a unique file identifier or common personal file identifier, except as authorized under subsection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



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1V8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca